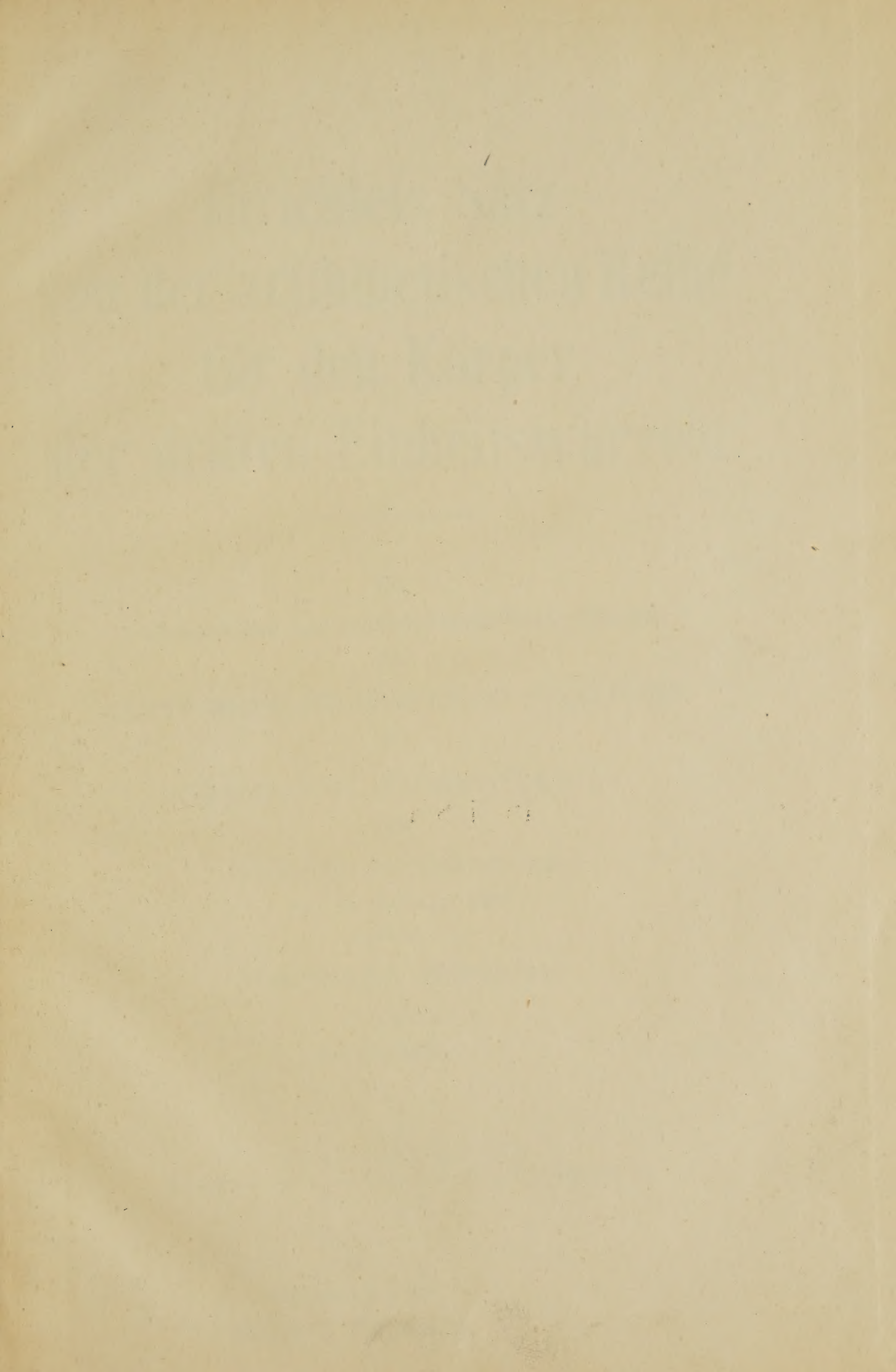
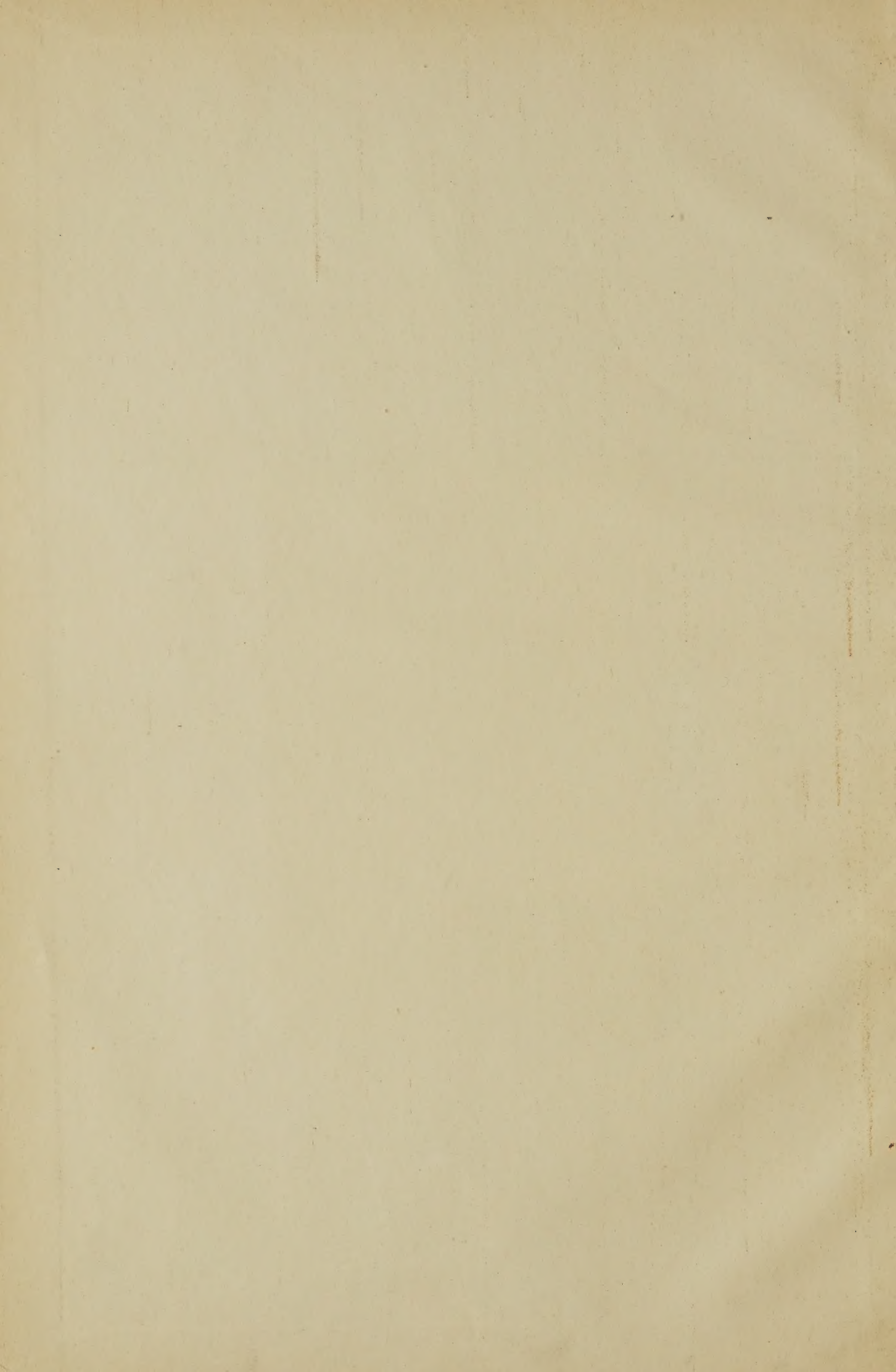
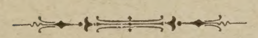




Dirichlets Satz von der arithmetischen Reihe für den Körper der dritten Einheitswurzeln

Der
mathematischen und naturwissenschaftlichen Fakultät
der
KAISER-WILHELMS-UNIVERSITÄT STRASSBURG
als
Inaugural-Dissertation
zur
Erlangung der Doktorwürde
am 25. Februar 1907
vorgelegt von

Hermann Bresslau
aus Berlin



STRASSBURG i. E.
Buchdruckerei C. & J. Gœller, Magdalenengasse 16
1907.

MEINEN ELTERN.

Einleitung.

Die vorliegende Arbeit schliesst sich an 3 Abhandlungen an, die Professor Weber in den Mathematischen Annalen veröffentlicht hat[1]. In den beiden ersten dieser Abhandlungen wird eine Reihe wichtiger Fragen über die Verteilung der Primzahlen und Primideale eines algebraischen Körpers untersucht und ihre Erledigung auf den Nachweis eines *Klassenkörpers* zurückgeführt. In der dritten Abhandlung wird dann gezeigt, wie sich für quadratische Körper mit negativer Diskriminante dieser Nachweis mit Hülfe der komplexen Multiplikation der elliptischen Funktionen führen lässt. Dabei werden jedoch der Gauss sche Zahlkörper und der Körper der dritten Einheitswurzeln, die einige Abweichungen zeigen, nur andeutungsweise

---

[1]) Ueber Zahlengruppen in algebraischen Zahlkörpern. Math. Ann., Bd. 48, 49, 50.

behandelt. In einer späteren Arbeit [1]) hat Herr Weber dann eine Durchführung der Untersuchungen für den Gaussschen Zahlkörper gegeben. Die entsprechende Behandlung des Körpers der dritten Einheitswurzeln soll im folgenden versucht werden.

Einen andersartigen Beweis des Dirichletschen Satzes für unseren Körper hat Herr Fanta im Anschluss an Arbeiten von Professor Mertens gegeben [2]).

---

[1]) Ueber komplexe Primzahlen in Linearformen. Journal f. reine u. angew. Math., Bd. 129.

[2]) Beweis, dass jede lineare Funktion, deren Koeffizienten dem kubischen Kreisteilungskörper entnommene ganze Zahlen sind, unendlich viele Primzahlen dieses Körpers darstellt. Monatshefte f. Math. u. Phys. 12. Jahrgang.

I. Die Primzahlen im Körper der dritten Einheitswurzeln.

§ I. Der Körper R (ρ)

Es sei R(ρ) der Körper der dritten Einheitswurzeln, der aus dem Körper R der rationalen Zahlen durch Adjunktion von

$$\rho = \frac{-1 + \sqrt{-3}}{2}$$

entsteht. Infolge der Identität

$$\rho^2 = -1 - \rho$$

sind alle Zahlen ξ dieses Körpers eindeutig darstellbar in der Form

$$\xi = x + y\rho,$$

worin x und y rationale Zahlen bedeuten. Sind x und y ausserdem auch noch ganze Zahlen, so ist ξ eine *ganze Zahl aus* R(ρ).

ξ ist eine Wurzel der Gleichung zweiten Grades

$$\xi^2 - (2x - y)\xi + (x^2 - xy + y^2) = 0,$$

deren absolutes Glied die *Norm von* ξ heisst:

$$N\xi = x^2 - xy + y^2 = \xi\xi',$$

wo

$$\xi' = x + y\rho^2 = (x - y) - y\rho$$

die *zu* ξ *konjugierte Zahl* bedeutet.

Sind ξ und η zwei Zahlen aus R (ρ), so ist

$$N\xi\eta = N\xi \; N\eta.$$

Die sechs Zahlen

$$\pm 1, \pm \rho, \pm \rho^2,$$

deren Norm die Zahl 1 ist, heissen die *Einheiten* von R (ρ), und je sechs Zahlen, die sich nur um Einheitsfaktoren von einander unterscheiden, wie

$$\pm \xi, \pm \rho\, \xi, \pm \rho^2\, \xi,$$

werden zu einander *assoziierte Zahlen* genannt.

Assoziierte Zahlen haben die gleiche Norm.

Da die rationalen Zahlen in R (ρ) selbst mit enthalten sind, müssen die Primzahlen dieses Körpers unter den Teilern der rationalen Primzahlen gesucht werden. Die Zahl 3 ist wegen der Identität

$$3 = -\rho^2 (1 - \rho)^2$$

mit dem Quadrate der Primzahl ($1-\rho$) assoziiert. Die rationalen Primzahlen

$$p \equiv 1 \text{ (mod. 3)}$$

können stets dargestellt werden durch einen Ausdruck von der Form

$$a^2 - a\, b + b^2$$

und sind folglich gleich dem Produkte der beiden Primzahlen

$$a + b\, \rho \text{ und } a + b\, \rho^2.$$

Solche in rationalen Primzahlen p enthaltenen komplexen Primzahlen aus R (ρ) sollen im folgenden mit π bezeichnet werden.

Es bleiben noch zu untersuchen die natürlichen Primzahlen

$$q \equiv 2 \text{ (mod. 3)}.$$

Da ein Ausdruck von der Form ($a^2 - ab + b^2$) niemals nach dem Modul 3 mit der Zahl 2 kongruent sein kann, sind die Zahlen q in R (ρ) nicht weiter zerlegbar und bleiben also auch in diesem Körper Primzahlen.

Die Primzahlen des Körpers $R(\rho)$ sind also durch die Typen

$$(1-\rho), \pi, q$$

erschöpft. Die Normen 3 und p der komplexen Primzahlen $(1-\rho)$ und π sind rationale Primzahlen, während die Normen der reellen Primzahlen q die Quadrate rationaler Primzahlen sind. Aus diesem Grunde nennt man die $(1-\rho)$ und π auch *Primzahlen ersten Grades*, zum Unterschiede von den *Primzahlen zweiten Grades* q.

§ 2. Die Verteilung der Primzahlen zweiten Grades.

Für die natürlichen Zahlen hat Dirichlet den Satz bewiesen:

In einer arithmetischen Reihe, deren Anfangsglied und Differenz zwei teilerfremde ganze Zahlen sind, kommen stets unendlich viele Primzahlen vor.

Wir wollen zunächst sehen, unter welchen Voraussetzungen sich dieser Satz auf die Primzahlen zweiten Grades von $R(\rho)$ übertragen lässt.

Es sei gegeben die Linearform

$$\lambda = \mu\xi + \alpha, \tag{1}$$

wo μ und α teilerfremde ganze Zahlen aus $R(\rho)$ sind, während ξ die Gesamtheit der ganzen Zahlen dieses Körpers durchläuft. Unter welchen Bedingungen sind dann in λ unendlich viele Primzahlen q enthalten?

Setzt man

$$\mu = m + n\rho \quad , \quad \alpha = a + b\rho \quad , \quad \xi = x + y\rho,$$

so folgt

$$\lambda = (mx - ny + a) + [n(x-y) + my + b]\rho;$$

damit nun in λ überhaupt reelle Zahlen enthalten sein

können, muss bei geeigneter Wahl der Zahlen x und y die Gleichung möglich sein

$$n(x - y) + m y + b = 0,$$

und dazu ist erforderlich und hinreichend, *dass der grösste gemeinsame Teiler* d *von* m *und* n *auch in* b *aufgeht.*

Unter dieser Voraussetzung sei ξ_0 irgend einer der Werte von ξ, für die λ reell wird.

Bezeichnet man nun die zu μ, ξ_0 und α konjugierten Zahlen bezw. mit μ', ξ'_0 und α', sodass also

$$(2) \qquad \mu \xi_0 + \alpha = \mu' \xi'_0 + \alpha' = \lambda_0$$

reell ist, so sind die sämtlichen Werte ξ^* von ξ, für die λ reell wird, in der Form enthalten:

$$\xi^* = \xi_0 + z \frac{\mu'}{d},$$

wo z die Reihe der ganzen rationalen Zahlen durchläuft. Setzt man diesen Ausdruck für ξ in (1) ein, so geht diese Formel über in

$$(3) \qquad \mu \xi^* + \alpha = \frac{\mu\mu'}{d} z + \lambda_0 = l,$$

und diese in λ enthaltene rationale Linearform l umfasst alle in λ vorkommenden rationalen Zahlen.

Die Primzahlen q genügen nun sämtlich der Kongruenz

$$q \equiv 2 \pmod{3}.$$

Damit solche Zahlen in l vorkommen können, muss demnach bei geeigneter Wahl von z die Kongruenz möglich sein

$$(4) \qquad l = \frac{\mu \mu'}{d} z + \lambda_0 \equiv 2 \pmod{3},$$

und dazu ist erforderlich und hinreichend, dass $(\lambda_0 + 1)$ durch den grössten gemeinsamen Teiler von $\frac{\mu \mu'}{d}$ und 3 teilbar sei, oder, was damit gleichbedeutend ist,

der grösste gemeinsame Teiler von μ *und* 3 *muss auch in* $(\alpha + 1)$ *aufgehen.*

Ist auch dieser Bedingung genügt und z_0 irgend einer der Werte von z, für die die Kongruenz (4) erfüllt ist, sodass also

$$(5) \qquad \frac{\mu \mu'}{d} z_0 + \lambda_0 = l_0 \equiv 2 \pmod{3}$$

wird, so sind alle übrigen Werte von z, für die (4) erfüllt ist, in der Form enthalten:

$$z^* = z_0 + 3\,t,$$

wo t die Reihe der natürlichen Zahlen durchläuft. Für die Werte z^* von z geht l über in

$$L = 3\frac{\mu \mu'}{d}\,t + l_0,$$

und diese in λ enthaltene rationale Linearform umfasst die sämtlichen in λ vorkommenden rationalen Zahlen, die nach dem Modul 3 mit der Zahl 2 kongruent sind. Unter diesen befinden sich nun nach dem Dirichletschen Satze unendlich viele Primzahlen — und zwar sind diese sämtlich von der Form q — falls die Zahlen l_0 und $3\frac{\mu\mu'}{d}$ teilerfremd sind.

Dass l_0 und 3 keinen gemeinsamen Teiler haben folgt aus (5), und wenn l_0 mit $\frac{\mu\mu'}{d}$ einen Teiler $\delta\delta'$ gemeinsam hätte, so ergäbe sich aus (5), dass auch λ_0 durch $\delta\delta'$ teilbar wäre, und dann würde nach (2) entweder δ oder δ' gemeinsamer Teiler von μ und α, während diese Zahlen doch als teilerfremd vorausgesetzt wurden.

Als Resultat unserer Untersuchung haben wir also den Satz erhalten:

Die Linearform $(\mu\,\xi + \alpha)$, *worin* $\mu = (m + n\,\rho)$ *und* $\alpha = (a + b\,\rho)$ *teilerfremde ganze Zahlen aus* $R(\rho)$ *be-*

deuten, während ξ *die Gesamtheit der ganzen Zahlen dieses Körpers durchläuft, stellt stets und nur dann unendlich viele Primzahlen zweiten Grades aus* R (ρ) *dar, wenn der grösste gemeinsame Teiler von* m *und* n *auch in* b, *derjenige von* μ *und* 3 *auch in* $\alpha + 1$ *aufgeht.*

§ 3. Die Zahlklassen nach dem Modul μ.

Es handelt sich nun noch um die in der Linearform

$$\lambda = \mu \xi + \alpha$$

enthaltenen Primzahlen π vom ersten Grade. Um nachzuweisen, dass λ unendlich viele solcher Primzahlen darstellt, wird, dem Gange der Dirichletschen Beweisführung entsprechend, zu zeigen sein, dass die über alle in λ enthaltenen Primzahlen π erstreckte Summe

$$\sum \frac{1}{N \pi}$$

unendlich wird; denn da sämtliche Glieder dieser Summe endliche Zahlen sind, folgt alsdann, dass die Anzahl der Summanden und demnach auch die Anzahl der Primzahlen π in λ unendlich gross ist.

Damit in λ überhaupt mehr als eine Primzahl vorkommen kann, müssen die Zahlen μ und α relativ prim sein. Solcher zu μ teilerfremder Zahlen α giebt es unendlich viele, und jede von ihnen giebt Anlass zur Bildung einer Linearform λ. Betrachtet man aber zwei solche Linearformen nur dann als von einander verschieden, wenn sie nicht dieselben Zahlen aus R (ρ) darstellen, so erhält man nur so viele verschiedene Linearformen λ, wie die Anzahl der nach dem Modul μ unter einander inkongruenten zu μ teilerfremden

Zahlen α beträgt. Diese Anzahl aber ist endlich, und zwar wird sie dargestellt durch das Produkt

$$\psi(\mu) = N\mu \prod \left(1 - \frac{1}{N\varkappa}\right),$$

das zu erstrecken ist über alle in μ enthaltenen Primzahlen $\varkappa$ vom ersten und vom zweiten Grade. [1])

Für alle Zahlen μ des Körpers $R(\rho)$, mit alleiniger Ausnahme von $\mu = 2$ und $\mu = (1 - \rho)$, sind die sechs Einheiten ε nach dem Modul μ unter einander inkongruent. Man kann daher unter den α eine endliche Anzahl $h = \frac{1}{6}\psi(\mu)$ so auswählen, dass jede zu μ teilerfremde Zahl mit einer der Zahlen

$$\varepsilon\alpha_1, \varepsilon\alpha_2, \quad . \quad . \quad . \quad . \quad , \varepsilon\alpha_h$$

nach dem Modul μ kongruent ist. Dann lassen sich die sämtlichen zu μ teilerfremden Zahlen in h Klassen

$$A_1, A_2, \quad . \quad . \quad . \quad . \quad , A_h$$

einteilen, indem alle Zahlen, die zu einer der Zahlen $\varepsilon\alpha_i$ nach dem Modul μ kongruent sind, in dieselbe Klasse A_i aufgenommen werden, sodass jede Zahl α in einer und nur einer dieser Klassen vorkommt. Gehört nun α_i in die Klasse A_i, so erhält man sämtliche Zahlen dieser Klasse, wenn man in den Linearformen

$$\mu\xi \pm \alpha_i \quad , \quad \mu\xi \pm \rho\alpha_i \quad , \quad \mu\xi \pm \rho^2\alpha_i$$

ξ die Gesamtheit der ganzen Zahlen von $R(\rho)$ durchlaufen lässt. Daraus folgt, dass es in jeder dieser Linearformen unendlich viele Primzahlen π giebt, wenn in A_i unendlich viele von ihnen enthalten sind. Denn jeder Primzahl π, die in A_i und folglich in einer dieser Linearformen enthalten ist, entspricht in jeder anderen Linearform der Klasse eine der zu π assoziierten Primzahlen.

---

[1]) Weber, Lehrbuch der Algebra, 2. Aufl., Bd. 2, § 168 (3).

Die beiden Ausnahmefälle $\mu = 1 - \rho$ und $\mu = 2$, für die unsere Klasseneinteilung nicht mehr ohne weiteres bestehen bleibt, brauchen wir im folgenden überhaupt nicht weiter berücksichtigen. Denn da sich in diesen Fällen alle zu μ teilerfremden ganzen Zahlen des Körpers in einer der Linearformen

$$(1 - \rho)\xi + 1 \; , \; (1 - \rho)\xi - 1 \qquad (\text{für } \mu = 1 - \rho)$$
$$2\xi + 1 \; , \; 2\xi + \rho \; , \; 2\xi + \rho^2 \qquad (\text{für } \mu = 2)$$

darstellen lassen, so erhalten wir in beiden Fällen nur eine einzige Klasse, und folglich sind in jeder dieser Linearformen unendlich viele Primzahlen π enthalten, falls es deren in $R(\rho)$ überhaupt unendlich viele giebt. Das ist aber sicher der Fall, denn nach dem Dirichletschen Satze existieren unendlich viele rationale Primzahlen der Form $p = (3n + 1)$ und von diesen zerfällt jede in zwei Primzahlen π. Wir können also im folgenden die Fälle $\mu = (1 - \rho)$ und $\mu = 2$, als schon erledigt, ausschliessen [1]).

§ 4. Die Summen $A_k(s) = \sum\limits^{\xi} \frac{1}{N\,\overline{\mu\,\xi + \alpha_k}^{\,s}}$.

Es sei A_k eine beliebige unter den Zahlklassen nach dem Modul μ und α_k ein Element aus A_k.

In der Linearform

$$\lambda_k = \mu\,\xi + \alpha_k$$

werden dann unendlich viele Zahlen aus A_k dargestellt.

[1]) Die Klassenzahl h wird ferner noch gleich 1 für $\mu = (1 + 3\rho)$, $\mu = 2(1 - \rho)$ und $\mu = 3$. Für diese Zahlen gilt also die gleiche Ueberlegung, sodass im folgenden $N\mu > 6$ angenommen werden darf.

Unter diesen ist aber nur eine endliche Anzahl $Z_k(n)$ von Zahlen, deren Norm eine gegebene positive ganze rationale Zahl n nicht überschreitet. Wenn wir nun

$$\alpha_k = \mu\,(a + b\,\rho)\ ,\ \xi = x + y\,\rho\ ,\ N\overline{\mu} = m$$

setzen, wo also m eine bestimmte ganze positive Zahl, a und b zwei feste rationale Brüche bedeuten, während x und y die Reihe der natürlichen Zahlen durchlaufen, so wird

$$N\overline{\mu\,\xi + \alpha_k} = m\,[(x+a)^2 - (x+a)(y+b) + (y+b)^2],$$

oder, wenn noch

$$x + a = x_1\ ,\ y + b = y_1$$

gesetzt wird,

$$N\overline{\mu\,\xi + \alpha_k} = m\,(x_1^2 - x_1\,y_1 + y_1^2).$$

Betrachten wir x_1 und y_1 als rechtwinklige Koordinaten einer Ebene, so erscheint diese mit einem Gitter überzogen, dessen quadratische Felder die Seite 1 haben. Jedes der Felder kann einem Gitterpunkte, etwa derjenigen seiner Ecken, deren Koordinaten den kleinsten Wert haben, eindeutig zugeordnet werden. Dann bedeutet $Z_k(n)$ die Anzahl der Gitterpunkte, die entweder im Inneren, oder auf der Kurve

$$x_1^2 - x_1\,y_1 + y_1^2 = \frac{n}{m}$$

gelegen sind. Diese Kurve ist eine Ellipse. Ihr Mittelpunkt ist der Koordinatenursprung, ihre Achsen haben die Länge $\sqrt{\frac{2\,n}{m}}$ und $\sqrt{\frac{2\,n}{3\,m}}$ und sind gegen die Koordinatenachsen um 45^0 gedreht. Die Quadrate, die zu den im Inneren der Ellipse gelegenen Gitterpunkten gehören, liegen ganz oder teilweise im Inneren der Ellipse, und umgekehrt gehören alle von der Kurve umschlossenen sowie ein Teil der von ihr durchschnittenen Felder zu Gitterpunkten, die innerhalb der

Ellipse liegen. Konstruieren wir nun zwei zu der ursprünglichen ähnliche und ähnlich liegende konzentrische Ellipsen, deren kleine Achsen um die Diagonale eines Quadrates, also um $\sqrt{2}$ kleiner bezw. grösser sind, als die der gegebenen, so umschliesst das von ihnen begrenzte ringförmige Flächenstück alle von der ursprünglichen Ellipse durchschnittenen Quadrate, und folglich ist der Flächeninhalt der innersten Ellipse kleiner, derjenige der äussersten Ellipse grösser, als die Gesamtfläche der Quadrate, deren Gitterpunkte innerhalb, oder auf der mittleren Ellipse liegen, d. h., es ist

$$\pi \sqrt{3}\left(\sqrt{\frac{2n}{3m}} - \sqrt{2}\right)^2 < Z_k(n) < \pi \sqrt{3}\left(\sqrt{\frac{2n}{3m}} + \sqrt{2}\right)^2,$$

oder

$$\frac{Z_k(n)}{n} = \frac{2\pi}{m\sqrt{3}} + \frac{M_k}{\sqrt{n}}, \tag{1}$$

wo

$$\frac{2\pi\sqrt{3}}{\sqrt{n}} - \frac{4\pi}{\sqrt{m}} < M_k < \frac{2\pi\sqrt{3}}{\sqrt{n}} + \frac{4\pi}{\sqrt{m}}.$$

Da nun $n \geqq 1$ und $m > 6$ ist, so ergiebt sich, dass M_k eine Funktion von m, n und der Klasse A_k ist, deren stets endlicher Wert innerhalb der Grenzen (-3) und $(+14)$ schwankt. Für unbegrenzt wachsendes n folgt also

$$\lim_{n=\infty} \frac{Z_k(n)}{n} = \frac{2\pi}{m\sqrt{3}},$$

und dieser Grenzwert ist von der besonderen Klasse A_k unabhängig, also für alle Klassen gleich.

Wir bilden jetzt die Summe

$$A_k(s) = \sum^{\xi} \frac{1}{\mathrm{N}\,\mu\,\xi + \alpha_k{}^s} \tag{2}$$

und ordnen ihre Glieder nach wachsenden Werten von $\mathrm{N}\,\mu\,\xi + \alpha_k$. Da $Z_k(n)$ die Anzahl der Zahlen

$(\mu\,\xi + \alpha_k)$ bezeichnet, deren Norm nicht grösser als n ist, so ergiebt sich

$$A_k(s) = \sum_{1,\infty}^{n} \frac{Z_k(n) - Z_k(n-1)}{n^s},$$

und hierin kann, solange $s \geqq 1$ ist, für $\frac{Z_k(n-1)}{n^s}$ auch geschrieben werden $\frac{Z_k(n)}{(n+1)^s}$, da $Z_k(0) = 0$ und

$$\lim_{n=\infty} \frac{Z_k(n) - Z_k(n-1)}{n^s} = \lim_{n=\infty} Z_k(n)\left[\frac{1}{n^s} - \frac{1}{(n+1)^s}\right] = 0.$$

Also ist

$$(3) \qquad A_k(s) = \sum_{1,\infty}^{n} Z_k(n)\left[\frac{1}{n^s} - \frac{1}{(n+1)^s}\right].$$

Wir formen zunächst den Klammerausdruck weiter um, indem wir setzen

$$(4) \quad \frac{1}{n^s} - \frac{1}{(n+1)^s} = \frac{s}{n^{s+1}} - \frac{1}{n^{s+1}(n+1)} - \frac{(s-1)}{n^{s+2}}\,\vartheta.$$

Hierin bedeutet ϑ eine Funktion von n und s,

$$\vartheta = n - \frac{n^3}{(n+1)(s-1)}\left[1 - \left(\frac{n}{n+1}\right)^{s-1}\right],$$

die für $n \geqq 1$ und $1 \leqq s < 2$ nur endliche Werte annimmt. Denn entwickeln wir

$$\left(\frac{n}{n+1}\right)^{s-1} = \left(1 - \frac{1}{n+1}\right)^{s-1}$$

nach dem binomischen Lehrsatze, so erhalten wir die Eingrenzung

$$1 - \frac{s-1}{n+1} - \frac{(s-1)(2-s)}{2(n+1)^2} \leqq \left(\frac{n}{n+1}\right)^{s-1} \leqq 1 - \frac{s-1}{n+1},$$

also für ϑ:

$$\frac{n}{n+1} + \frac{n^2}{(n+1)^2} - \frac{2-s}{2}\,\frac{n^3}{(n+1)^3} \leqq \vartheta \leqq \frac{n}{n+1} + \frac{n^2}{(n+1)^2},$$

d. h. ϑ liegt für $n \geqq 1$ und $1 \leqq s < 2$ zwischen den Grenzen $^3/_4$ und 2.

Führen wir nun in (3) die Werte von $Z_k(n)$ und

$$\left[\frac{1}{n^s} - \frac{1}{(n+1)^s}\right]$$

nach (1) und (4) ein, so erhalten wir:

$$A_k(s) = \frac{2\pi s}{m\sqrt{3}} \sum \frac{1}{n^s} - \frac{2\pi}{m\sqrt{3}} \sum \frac{1}{n^s(n+1)}$$
$$- \frac{2\pi(s-1)}{m\sqrt{3}} \sum \frac{\vartheta}{n^{s+1}} + s \sum \frac{M_k}{n^{s+\frac{1}{2}}} - \sum \frac{M_k}{n^{s+\frac{1}{2}}(n+1)}$$
$$- (s-1) \sum \frac{M_k \vartheta}{n^{s+3/2}},$$

oder

$$A_k(s) - \frac{2\pi}{m(s-1)\sqrt{3}} = \frac{2\pi}{m\sqrt{3}}\left[-\frac{1}{s-1} + \sum \frac{1}{n^s}\right]$$
$$+ \frac{2\pi(s-1)}{m\sqrt{3}} \sum \frac{1}{n^s} - \frac{2\pi}{m\sqrt{3}} \sum \frac{1}{n^s(n+1)}$$
$$- \frac{2\pi(s-1)}{m\sqrt{3}} \sum \frac{\vartheta}{n^{s+1}} + s \sum \frac{M_k}{n^{s+\frac{1}{2}}}$$
$$- \sum \frac{M_k}{n^{s+\frac{1}{2}}(n+1)} - (s-1) \sum \frac{M_k \vartheta}{n^{s+3/2}},$$

wo sämtliche Summen über n von 1 bis ∞ zu erstrecken sind.

Solange $s > 1$ ist, konvergieren alle diese Dirichletschen Summen. Lassen wir nun s in 1 übergehen, so wird

$$\lim \left[-\frac{1}{s-1} + \sum \frac{1}{n^s}\right] = C = 0{,}5772 \;\cdot\;\cdot$$

(= der Eulerschen Konstanten),

$$\lim (s-1) \sum \frac{1}{n^s} = \lim 1 + (s-1)\left[-\frac{1}{s-1} + \sum \frac{1}{n^s}\right] = 1,$$

$$\lim \sum \frac{1}{n^s(n+1)} = \sum \frac{1}{n(n+1)} = \lim_{n=\infty} \frac{n}{n+1} = 1,$$

und auch die übrigen Summenausdrücke konvergieren für $s = 1$ gegen bestimmte endliche Werte. Demnach ergiebt sich

$$\lim_{s=1} A_k(s) - \frac{2\pi}{m(s-1)\sqrt{3}} = \frac{2\pi}{m\sqrt{3}} C + \sum_{1,\infty}^{n} \frac{M_k}{\sqrt{n(n+1)}},$$

und dies ist eine bestimmte endliche Zahl, die nur von m und der betreffenden Klasse abhängt. Setzen wir also

$$A_k(s) = \frac{2\pi}{m(s-1)\sqrt{3}} + G_k(s), \tag{5}$$

so ist G_k eine Funktion von s, die für $1 \leq s < 2$ bestimmte endliche Werte annimmt.

§ 5. Die Verteilung der Primzahlen ersten Grades.

Die Zahlklassen nach dem Modul μ lassen sich auffassen als Elemente einer Abelschen Gruppe $\mathfrak{A}$. Denn sind A_i und A_k zwei beliebige unter den Klassen und α_i und α_k irgend zwei Zahlen aus A_i bezw. A_k, so gehört das Produkt $\alpha_i \alpha_k$ wieder einer ganz bestimmten Klasse A_l an, und diese *aus* A_i *und* A_k *komponierte* Klasse A_l hängt nur ab von der Wahl der ursprünglichen Klassen A_i und A_k, nicht aber von der Auswahl der Zahlen α_i und α_k aus diesen Klassen. Einheitselement der Gruppe $\mathfrak{A}$ ist die *Hauptklasse* A_1, die alle nach dem Modul μ zu einer der sechs Einheiten ε des Körpers kongruenten Zahlen enthält.

Zu der Gruppe $\mathfrak{A}$ gehören h *Charaktere* [1])

$$\chi_1, \chi_2, \cdots\cdots \chi_h,$$

[1]) Algebra, Bd. 2, § 13.

die eine zu $\mathfrak{A}$ isomorphe Gruppe bilden. Die Charaktere sind für alle Elemente der Gruppe $\mathfrak{A}$ h^{te} Einheitswurzeln, der *Hauptcharakter* χ_1 ist für jedes A gleich 1.

Ferner ist

$$(1) \qquad \sum_{1,\,h}^{k} \chi_i\,(A_k) = h, \text{ oder } = 0$$

je nachdem $i = 1$, oder $\neq 1$ ist und

$$(2) \qquad \sum_{1,\,h}^{i} \chi_i\,(A_k) = h, \text{ oder } = 0$$

je nachdem $k = 1$, oder $\neq 1$ ist.

Wir bilden nun die Summe

$$Q_i\,(s) = \sum_{1,\,h}^{k} A_k\,(s)\;\chi_i\,(A_k).$$

Nach § 4 (5) wird dann

$$Q_i\,(s) = \frac{2\,\pi}{m\,(s-1)\sqrt{3}} \sum_{1,\,h}^{k} \chi_i\,(A_k) + \sum_{1,\,h}^{k} \chi_i\,(A_k) \cdot G_k(s),$$

also wegen (1)

$$Q_1\,(s) = \frac{2\,\pi\,h}{n\,(s-1)\sqrt{3}} + \sum_{1,\,h}^{k} G_k\,(s),$$

$$Q_i\,(s) = \sum_{1,\,h}^{k} \chi_i\,(A_k)\;G_k\,(s) \qquad (i = 2, 3, \ldots h).$$

Nähert sich jetzt s dem Genzwerte 1, so gehen nach den Darlegungen des vorigen Paragraphen die Ausdrücke

$$\lim_{s=1}\,(s-1)\,Q_1\,(s),\; Q_2\,(s),\; Q_3\,(s),\; \ldots,\; Q_h\,(s)$$

in ganz bestimmte endliche Werte über. Wenn wir

nun den *Charakter einer zu* μ *teilerfremden Zahl* α durch die Gleichung definieren

$$\chi_i(\alpha) = \chi_i(A),$$

wo A die Klasse bedeutet, der α angehört, so können wir setzen

$$Q_i(s) = \sum^{\alpha} \frac{\chi_i(\alpha)}{\overline{N\alpha}^{\,s}},$$

die Summe erstreckt über alle zu μ teilerfremden Zahlen α des Körpers, jedoch so, dass von je sechs assoziierten Zahlen immer nur eine in die Summe aufgenommen wird.

Die Summen Q sind, solange s grösser als 1 ist, unbedingt konvergent und dasselbe gilt, wenn $\varkappa$ eine beliebige nicht in μ enthaltene Primzahl (ersten oder zweiten Grades) aus $R(\rho)$ bedeutet, von der Summe

$$S_\varkappa = 1 + \frac{\chi_i(\varkappa)}{\overline{N\varkappa}^{\,s}} + \frac{\chi_i(\varkappa^2)}{\overline{N\varkappa^2}^{\,s}} + \ldots,$$

die ein Teil von $Q_i(s)$ ist. Da nun

$$\chi_i(ab) = \chi_i(a)\,\chi_i(b)$$

und

$$\overline{Nab} = \overline{Na}\;\overline{Nb},$$

so wird

$$S_\varkappa = 1 + \left(\frac{\chi_i(\varkappa)}{\overline{N\varkappa}^{\,s}}\right) + \left(\frac{\chi_i(\varkappa)}{\overline{N\varkappa}^{\,s}}\right)^2 + \ldots,$$

oder

$$S_\varkappa = \frac{1}{1 - \chi_i(\varkappa)\,\overline{N\varkappa}^{\,-s}}.$$

Lassen wir $\varkappa$ die Gesamtheit der nicht in μ aufgehenden Primzahlen aus $R(\rho)$ durchlaufen, mit der Einschränkung, dass von je sechs assoziierten Primzahlen immer nur eine aufgenommen wird, so folgt

$$Q_i(s) = \prod^{\varkappa} S_\varkappa = \prod^{\varkappa} \frac{1}{1 - \chi_i(\varkappa)\,\overline{N\varkappa}^{\,-s}}.$$

Hieraus findet sich nach der Formel

$$\log \frac{1}{1-z} = z + \frac{z^2}{2} + \frac{z^3}{3} + \dots$$

die Reihenentwicklung

$$(3) \quad \log Q_i(s) = \sum^{\varkappa} \frac{\chi_i(\varkappa)}{N\varkappa^{s}} + \frac{1}{2} \sum^{\varkappa} \frac{\chi_i(\varkappa^2)}{N\varkappa^{2s}} + \dots$$

Die Summen auf der rechten Seite ändern sich stetig mit s, solange nur $s > 1$ bleibt, und folglich ist durch (3) der Logarithmus von $Q_i(s)$ bis auf ein konstantes Vielfaches von $2\pi i$ bestimmt.

In der Gruppe $\mathfrak{A}$ giebt es zu jeder Klasse A eine *reziproke* Klasse $\bar{A}$, sodass, wenn α eine Zahl aus A, $\bar{\alpha}$ eine Zahl aus $\bar{A}$ bedeutet, das Produkt $\alpha\bar{\alpha}$ der Hauptklasse A_1 angehört. Bilden wir nun die Summe

$$\frac{1}{h} \sum_{1,\,h}^{i} \chi_i(\bar{\alpha}) \log Q_i(s),$$

so ergiebt sich nach (2)

$$(4) \quad \frac{1}{h} \sum_{1,\,h}^{i} \chi_i(\bar{\alpha}) \log Q_i(s) = \sum^{\varkappa} \frac{1}{N\varkappa^{s}} + \frac{1}{2} \sum^{\varkappa} \frac{1}{N\varkappa^{2s}} + \dots$$

worin sich die 1te, 2te, ... Summe auf der rechten Seite über alle die Primzahlen erstreckt, deren 1te, 2te, ... Potenz in der Linearform

$$\lambda = \mu\,\xi + \alpha$$

enthalten ist. Die erste dieser Summen zerlegen wir in zwei Teile

$$S = \sum^{\pi} \frac{1}{N\pi^{s}} \quad \text{und} \quad S_1 = \sum^{q} \frac{1}{q^{2s}},$$

indem wir in S alle in λ enthaltenen Primzahlen ersten Grades π, in S_1 die Primzahlen zweiten Grades q aufnehmen. In den folgenden Summen

$$S_2 = \sum^{\varkappa} \frac{1}{N\overline{\varkappa}^{2s}}, \quad S_3 = \sum^{\varkappa} \frac{1}{N\overline{\varkappa}^{3s}}, \dots$$

ist eine solche Zerlegung nicht nötig. Die ganze Summenreihe

$$T = \tfrac{1}{2} S_2 + \tfrac{1}{3} S_3 + \dots.$$

bleibt für $s \geqq 1$ endlich. Denn vergrössern wir alle Summen, indem wir sie über sämtliche Primzahlen aus $R(\rho)$ erstrecken, so folgt

$$T < \frac{1}{2}\left[\sum \frac{1}{N\overline{\varkappa}^{2s}} + \sum \frac{1}{N\overline{\varkappa}^{3s}} + \dots\right] = \frac{1}{2} \sum \frac{1}{N\overline{\varkappa}^{2s} - N\overline{\varkappa}^{s}}$$

Die Zahlen $N\overline{\varkappa}$ sind rationale Primzahlen, oder Quadrate von rationalen Primzahlen, und keine von diesen kann öfter als zweimal vorkommen. Es wird also um so mehr

$$T < \sum_{3,\infty}^{n} \frac{1}{n^{2s}\left(1 - \frac{1}{n^s}\right)}$$

oder, da

$$1 - \frac{1}{n^s} > \frac{1}{3},$$

$$T < 3 \cdot \sum \frac{1}{n^{2s}},$$

und diese Summe hat einen endlichen Wert.

Auf der linken Seite von (4) wird Q_1 für $s = 1$ unendlich, während $Q_2, Q_3, \dots Q_h$ endllch bleiben. Wenn wir nun ausserdem noch beweisen können, dass diese letzteren Summen für $s = 1$ von Null verschiedene Werte annehmen, so folgt, dass die linke Seite der Gleichung (4) für $s = 1$ unendlich wird.

Auf der rechten Seite von (4) bleibt für $s = 1$ die Summenreihe

$$S_1 + \tfrac{1}{2} S_2 + \tfrac{1}{3} S_3 + \dots$$

endlich, wenn also die linke Seite unendlich wird, so folgt

$$\lim_{s=1} S = \sum^{\pi} \frac{1}{N\pi} = \infty \ ,$$

wo die Summe S über alle in der Linearform λ enthaltenen Primzahlen ersten Grades π zu erstrecken ist. Damit aber wäre, wie wir am Anfange von § 3 sahen, der Beweis vollendet.

§ 6. Der Klassenkörper.

Um unseren Beweis zu Ende zu führen, müssen wir nun noch zeigen, dass die Grenzwerte der Summen

$$Q_2(s), Q_3(s), \ldots . Q_h(s)$$

für $s = 1$ von Null verschieden sind. Zu diesem Zwecke bilden wir das Produkt

$$Q_1(s)\, Q_2(s) \ldots Q_h(s) = \prod_{1,\, h}^{i} \prod^{\varkappa} \frac{1}{1 - \chi_i(\varkappa)\, N\varkappa^{-s}} .$$

Eine jede Primzahl $\varkappa$ gehört nach dem Modul μ zu einem bestimmten Exponenten $a_\varkappa$, d. h. es giebt eine kleinste positive Zahl $a_\varkappa$, sodass $\varkappa^{a_\varkappa}$ in die Hauptklasse nach dem Modul μ gehört. $a_\varkappa$ ist ein Teiler von h

$$h = a_\varkappa \cdot b_\varkappa .$$

Die h Charaktere $\chi_i(\varkappa)$ sind dann sämtlich $a_\varkappa$^te Einheitswurzeln, von denen jede gleich oft, also $b_\varkappa$-mal unter den $\chi_i(\varkappa)$ vorkommt. Folglich wird

$$\prod_{1,h}^{i} \frac{1}{1 - \chi_i(\varkappa) N\varkappa^{-s}} = \frac{1}{(1 - N\varkappa^{-a_\varkappa s})^{b_\varkappa}}$$

und

$$\prod^{i} Q_i(s) = \prod^{\varkappa} \frac{1}{(1 - N\varkappa^{-a_\varkappa s})^{b_\varkappa}}.$$

Dies Produkt zerlegen wir in zwei Teilprodukte. In das erste nehmen wir alle die Primzahlen ersten Grades π auf, die nach dem Modul μ zum Exponenten 1 gehören, in das zweite alle übrigen Primzahlen ersten und die sämtlichen Primzahlen zweiten Grades. Setzen wir demgemäss

$$P_1 = \prod^{\pi} \frac{1}{1 - N\pi^{-s}}, \quad P_2 = \prod^{\varkappa} \frac{1}{(1 - N\varkappa^{-a_\varkappa s})^{b_\varkappa}},$$

so wird

$$\prod^{i} Q_i(s) = P_1^{h} \cdot P_2.$$

Das Produkt P_2 ist von Null verschieden, weil keiner seiner Faktoren kleiner als 1 ist. Es kann aber auch für $s \geqq 1$ nicht unendlich werden, weil es sicher kleiner ist, als die für $s \geqq 1$ gegen einen endlichen Grenzwert konvergierende Summe

$$\left(\sum_{1,\infty}^{n} \frac{1}{n^{2s}}\right)^{\frac{h}{2}}.$$

Nun ist

$$\lim_{s=1} (s - 1) Q_1(s) Q_2(s) \ldots Q_h(s) = \lim_{s=1} (s - 1) P_1^{h} P_2$$

endlich, und folglich muss auch $(s - 1) P_1^{h}$ für $s = 1$ einen endlichen Grenzwert haben. Um jetzt noch nachzuweisen, dass von den Summen $Q_2(s), Q_3(s), \ldots, Q_h(s)$ keine für $s = 1$ verschwindet, genügt es nach unserer

letzten Gleichung, wenn wir zeigen können, dass die Ungleichung besteht

$$\lim_{s=1} (s - 1) P_1^h \neq 0.$$

Dieser letzte uns noch übrig bleibende Beweis lässt sich dadurch erbringen, dass wir die Existenz eines algebraischen Zahlkörpers Ω über $R(\rho)$ nachweisen, der die folgenden Eigenschaften hat:

1. *Der Relativgrad* n *von* Ω *über* $R(\rho)$ *ist nicht grösser als* h.
2. *Jede Primzahl ersten Grades* π, *die nach dem Modul* μ *zum Exponenten* 1 *gehört, zerfällt in* Ω *in lauter Primideale ersten Grades* $\mathfrak{p}$.
3. *Alle übrigen Primzahlen* $\varkappa$ *aus* $R(\rho)$ *sind in* Ω *nur in Primfaktoren von höherem, als dem ersten Grade zerlegbar.*
4. *Von den Bedingungen 2. und 3. kann eine endliche Anzahl Primzahlen ausgenommen sein.*

Ein Körper Ω, der diesen Bedingungen genügt, heisst ein *Klassenkörper über* $R(\rho)$ *nach dem Modul* μ. Haben wir seine Existenz nachgewiesen, so können wir uns zur Vollendung unseres Beweises auf den folgenden Satz stützen, der allgemein für jeden algebraischen Zahlkörper Ω gültig ist: [1])

Durchläuft $\mathfrak{p}$ *die Gesamtheit der Primideale ersten Grades in einem algebraischen Körper* Ω, *so hat das Produkt*

$$(s - 1) \prod \frac{1}{1 - N_\Omega \, \mathfrak{p}^{-s}}$$

für $s = 1$ *einen endlichen, von Null verschiedenen Grenzwert.*

---

[1]) Algebra, Bd. 2, § 197 I.

Das Zeichen N_{Ω} bedeutet die im Körper Ω genommene Norm. Erfüllt nun Ω die Bedingungen 1. bis 4., so wird

$$N_{\Omega}\,\pi = N\pi^{\,n}$$

$$N_{\Omega}\,\mathfrak{p} = N\pi\ ,$$

und π zerfällt in n von einander verschiedene Primideale ersten Grades

$$\mathfrak{p}_1,\ \mathfrak{p}_2,\ \ldots\ldots,\ \mathfrak{p}_n\,.$$

Eine Ausnahme machen nur diejenigen Primideale ersten Grades, die in höherer, als der ersten Potenz in Primzahlen des Körpers $R(\rho)$ aufgehen. Diese sind aber sämtlich in der Diskriminante des Körpers Ω enthalten und folglich nur in endlicher Anzahl vorhanden. Wir können sie deshalb fortlassen, ohne dass die Bündigkeit unseres Beweises darunter leidet, denn wir haben es hier mit unendlichen Produkten P zu tun, deren sämtliche Faktoren endliche Zahlen grösser als 1 sind, und es kann daher das Fortlassen einer endlichen Anzahl solcher Faktoren an dem Verschwinden, oder Nichtverschwinden des Grenzwertes

$$\lim_{s=1}\,(s-1)\,P$$

nicht das mindeste ändern. Demnach wird bis auf einen endlichen, von Null verschiedenen Faktor

$$\prod \frac{1}{1 - N_{\Omega}\,\mathfrak{p}^{\,-s}} = \prod \frac{1}{(1 - N\pi^{\,-s})^n} = P_1^{\,n}$$

und folglich besitzt

$$\lim_{s=1}\,(s-1)\,P_1^{\,n}$$

einen endlichen von Null verschiedenen Wert. Andrerseits war auch

$$\lim_{s=1}\,(s-1)\,P_1^{\,h}$$

endlich, und folglich muss auch P_1^{h-n} endlich sein. Da aber P_1 selber unendlich ist, kann das nur dann eintreten, wenn

$$h = n.$$

Damit ist dann der Beweis, dass

$$\lim_{s=1} (s-1) P_1^h$$

von Null verschieden ist, geführt und der Dirichletsche Satz für den Körper der dritten Einheitswurzeln bewiesen. Dem Nachweise des Klassenkörpers, dessen Existenz wir bei unseren letzten Schlussfolgerungen voraussetzten, ist der zweite Teil dieser Arbeit gewidmet.

II. Die komplexe Multiplikation der elliptischen Funktionen mit dem Periodenverhältnis $\omega = \rho$.

§ 7. Die Weierstrasssche $\wp$-Funktion.

Wir betrachten die Weierstrasssche $\wp$-Funktion für den besonderen Fall, dass das Verhältnis ω ihrer Perioden ω_1 und ω_2 gleich der dritten Einheitswurzel ρ ist:

$$\omega = \frac{\omega_2}{\omega_1} = \rho .$$

Wenn nun $\mu = x + y\rho$ eine Zahl aus $R(\rho)$ bedeutet, so wird

$$\begin{aligned} \mu\,\omega_1 &= x\,\omega_1 + y\,\omega_2 \\ \mu\,\omega_2 &= -\,y\,\omega_1 + (x - y)\,\omega_2 . \end{aligned} \tag{1}$$

$\mu\omega_1$ und $\mu\omega_2$ sind also stets und nur dann gleichfalls Perioden von $\wp(u)$, wenn μ als *ganze* Zahl angenommen wird. Ist dies der Fall, so folgt weiter, dass $\wp(\mu u)$ gleichfalls eine doppeltperiodische Funktion von u mit den Perioden ω_1 und ω_2 ist. Denn verstehen wir unter h_1 und h_2 irgend welche ganzen rationalen Zahlen, so ist

$$\wp[\mu(u + h_1\omega_1 + h_2\omega_2)]$$
$$= \wp[\mu u + (h_1 x - h_2 y)\omega_1 + (h_1 y + h_2 x - h_2 y)\omega_2] = \wp(\mu u).$$

Da ferner $\wp(u)$ eine gerade Funktion von u ist, gilt dasselbe auch von $\wp(\mu u)$, und diese Funktion lässt sich deshalb als rationale Funktion von $\wp(u)$ darstellen [1]). Wir können etwa ansetzen

$$\wp(\mu u) = \frac{G_\mu}{\Gamma_\mu}$$

wo G_μ und Γ_μ zwei teilerfremde ganze rationale Funktionen von $\wp(u)$ bedeuten sollen, deren Eigenschaften wir jetzt näher untersuchen müssen.

Für $\wp(u)$ gilt allgemein in der Umgebung des Nullpunktes die Reihenentwicklung [2])

$$\wp(u) = \sum_{0,\ \infty}^{\lambda} c_\lambda \, u^{2\lambda - 2},$$

worin

$$c_0 = 1,\ c_1 = 0,\ c_2 = \frac{g_2}{20},\ c_3 = \frac{g_3}{28}$$

und, für $\lambda > 3$,

$$c_\lambda = \frac{3}{(\lambda - 3)(2\lambda + 1)} \sum_{2,\lambda-2}^{\nu} c_\nu \, c_{\lambda - \nu},$$

also die c_λ sämtlich ganze Funktionen mit rationalen Koeffizienten der *Weierstrassschen Invarianten* g_2 und g_3 sind.

Für unser spezielles Periodenverhältnis lässt sich diese Reihenentwicklung vereinfachen. Die $\wp$-Funktion ist gegenüber linearen Transformationen ihrer Perioden invariant. Substituieren wir nun für ω_1 und ω_2 die Werte $\rho\omega_1$ und $\rho\omega_2$, so wird nach (1)

---

[1]) Schwarz-Weierstrass, Formeln und Lehrsätze zum Gebrauche der elliptischen Funktionen, 14.

[2]) Formeln und Lehrsätze, 9.

$$\rho\omega_1 = 0 \cdot \omega_1 + 1 \cdot \omega_2,$$
$$\rho\omega_2 = -1 \cdot \omega_1 - 1\, \omega_2,$$

die Determinante dieser Substitution also gleich 1, d. h. unsere Transformation ist linear, und es ist

$$\wp\,(\rho u, \rho\omega_1, \rho\omega_2) = \wp\,(\rho u, \omega_1, \omega_2).$$

Andrerseits gilt [1]), wenn λ irgend einen Parameter bedeutet, die Gleichung

$$\wp\,(\lambda u, \lambda\omega_1, \lambda\omega_2) = \lambda^{-2}\,\wp\,(u, \omega_1, \omega_2),$$

und wenn wir $\lambda = \rho$ setzen, ergiebt sich aus den beiden letzten Formeln

$$(3) \qquad \wp\,(u) = \rho^2\,\wp\,(\rho u) = \rho\,\wp\,(\rho^2 u).$$

Setzen wir hier $u = \frac{\omega_1}{2}$, so wird $\rho u = \frac{\omega_2}{2}$ und $\rho^2 u = -\frac{\omega_1 + \omega_2}{2}$, also folgt, wenn wir zur Abkürzung setzen

$$\wp\left(\frac{\omega_1}{2}\right) = e_1,\ \wp\left(\frac{\omega_2}{2}\right) = e_2,\ \wp\left(\frac{\omega_1 + \omega_2}{2}\right) = e_3,$$

$$e_1 = \rho^2\, e_2 = \rho\, e_3.$$

Durch e_1, e_2 und e_3 lassen sich die Weierstrassschen Invarianten berechnen nach den Formeln [2])

$$(4) \quad \begin{aligned} g_2 &= -4\,(e_1 e_2 + e_2 e_3 + e_3 e_1) = -4\, e_1^2 (1 + \rho + \rho_2) = 0, \\ g_3 &= 4\, e_1\, e_2\, e_3 = 4\, e_1^3\, \rho^3 = 4\,\wp^3\left(\frac{\omega_1}{2}\right). \end{aligned}$$

In der obigen Reihenentwicklung für $\wp\,(u)$ verschwinden also alle Glieder, die g_2 als Faktor enthalten, und die Reihe nimmt die Gestalt an

$$(5) \qquad \wp\,(u) = \sum_{0,\,\infty}^{\lambda} a_\lambda\, g_3^\lambda\, u^{6\lambda - 2},$$

---

[1]) Weber, Elliptische Funktionen und algebraische Zahlen, § 41.

[2]) Elliptische Funktionen, § 41.

$$\text{wo } a_0 = 1,\ a_1 = \frac{1}{28} \text{ und, für } \lambda > 1,$$

$$a_\lambda = \frac{1}{(6\lambda + 1)(\lambda - 1)} \sum_{1,\lambda-1}^{\lambda} a_\nu\, a_{\lambda-\nu}$$

ist, die a_λ also sämtlich rationale Zahlen sind. Es wird demnach

$$\frac{\wp(\mu u)}{\wp(u)} = \mu^{-2} \frac{\sum a_\lambda\, g_3^\lambda\, (\mu u)^{6\lambda}}{\sum a_\lambda\, g_3^\lambda\, u^{6\lambda}},$$

und folglich nach (2)

$$\lim_{u=0} \frac{G_\mu}{\Gamma_\mu \cdot \wp(u)} = \mu^{-2}.$$

Da nun nach (5) $\wp(u)$ für $u = 0$ zur zweiten Ordnung unendlich wird, während $G_\mu : \Gamma_\mu \wp(u)$ endlich bleibt, so ergiebt sich, *dass* G_μ *eine um einen Grad höhere Funktion des Argumentes* $\wp(u)$ *ist, als* Γ_μ. Die Werte

$$u \equiv 0 \pmod{\omega_1, \omega_2}$$

sind die einzigen, für die die ganzen rationalen Funktionen G_μ und Γ_μ von $\wp(u)$ überhaupt unendlich werden können. Alle übrigen Unstetigkeitsstellen von $\wp(\mu u)$ müssen deshalb zugleich die Nullstellen von Γ_μ sein. Als Wurzeln von Γ_μ ergeben sich also die Werte, die $\wp(\mu u)$ annimmt, wenn μu, aber nicht auch u selbst eine Periode wird, d. h. die Grössen

$$\gamma_{\nu/\mu} = \wp\left(\frac{h_1\,\omega_1 + h_2\,\omega_2}{\mu}\right) = \wp\left(\frac{\nu}{\mu}\,\omega_1\right),$$

wo $\nu = (h_1 + h_2\,\rho)$ eine ganze, nicht durch μ teilbare Zahl aus $R(\rho)$ bedeutet. Da nun $\wp(\mu u)$ immer zur zweiten Ordnung unendlich wird, kommen in Γ_μ alle die Faktoren $(\wp(u) - \gamma_{\nu/\mu})$ zweimal vor, mit Ausnahme

derjenigen, die für $u = \frac{\nu}{\mu}\,\omega_1$ zur zweiten Ordnung verschwinden, für die also auch $\wp'(u)$ gleich Null wird. Das tritt aber stets und nur dann ein, wenn $\frac{\nu}{\mu}\,\omega_1$ eine halbe Periode ist, d. h. sobald

(6) $$2\,\nu \equiv 0 \ (\text{mod. } \mu).$$

Für zwei verschiedene Zahlen ν und ν' werden die Werte $\gamma_{\nu/\mu}$ und $\gamma_{\nu'/\mu}$ dann und nur dann einander gleich, wenn

$$\nu \equiv \nu' \ (\text{mod. } \mu).$$

Demnach können wir die Primfaktoren von Γ_μ folgendermassen bestimmen:

Ist μ nicht durch 2 teilbar, so sind die Werte $+\nu$ und $-\nu$ unter einander nach dem Modul μ inkongruent und Γ_μ hat folglich $\frac{m-1}{2}$ unter einander verschiedene Wurzeln, von denen jede zweimal vorkommt. Dabei ist $N\mu$ zur Abkürzung gleich m gesetzt worden.

Ist dagegen μ durch 2 teilbar, so hat die Kongruenz (6) ausser $\nu = 0$ noch drei andere unter einander inkongruente Lösungen, denen die Werte $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ und $\frac{\omega_1 + \omega_2}{2}$ von $\frac{\nu}{\mu}\,\omega_1$ entsprechen. Also hat in diesem Falle Γ_μ ausser $\frac{m-4}{2}$ doppelten noch die drei einfachen Wurzeln e_1, e_2, e_3, und diese sind zugleich die Nullstellen der Funktion

$$4\,\wp^3(u) - g_3,$$

die also als Faktor in Γ_μ vorkommt.

Ferner sind für jeden ganzzahligen Modul μ aus $R(\rho)$ die Zahlen ν, $\rho\nu$ und $\rho^2\nu$ unter einander inkongruent. Ausgenommen ist hierbei nur der Modul $\mu = (1 - \rho)$, doch ordnet sich auch dieser Fall der im

folgenden aufgestellten Regel unter. Es lassen sich also die doppelten Wurzeln der Gleichung $\Gamma_\mu = 0$ zu je dreien ordnen, wie

$$\gamma_{\nu/\mu}, \qquad \gamma_{\nu\varrho/\mu} = \rho^2 \gamma_{\nu/\mu}, \qquad \gamma_{\nu\varrho^2/\mu} = \rho \gamma_{\nu/\mu},$$

und können demnach als Wurzeln einer Gleichung

$$\wp^3(u) - \gamma^3_{\nu/\mu} = 0$$

zusammengefasst werden. Nur dann ist eine solche Zusammenfassung unstatthaft, wenn die Grössen $\gamma_{\nu/\mu}$, $\gamma_{\nu\varrho/\mu}$, $\gamma_{\nu\varrho^2/\mu}$ alle drei verschwinden. Das ist aber nur möglich, wenn

$$u \equiv \pm \rho u \equiv \pm \rho^2 u$$

werden kann, und aus dieser Kongruenz ergiebt sich, ausser dem als Lösung unzulässigen Wert $u \equiv 0$, die Bedingungsgleichung

$$u = \frac{\varkappa}{1 - \rho} \omega_1,$$

wo $\varkappa$ eine nicht durch $(1 - \rho)$ teilbare ganze Zahl aus $R(\rho)$ bedeutet. Es muss demnach, wenn der Wert Null unter den Wurzeln von Γ_μ vorkommt, die Zahl μ durch $(1 - \rho)$ teilbar sein.

Die Resultate unserer Untersuchung von Γ_μ fassen wir in dem folgenden Satze zusammen:

Γ_μ ist eine ganze rationale Funktion des Argumentes $\wp(u)$ vom Grade $(m - 1)$, und zwar ist diese Funktion von der Form

$$\Gamma_\mu = [4\wp^3(u) - g_3]\cdot[\wp(u)\Gamma^*_\mu]^2, \text{ wenn } \mu \equiv 0 \pmod{2} \text{ und } \mu \equiv 0 \pmod{1 - \rho},$$
$$\Gamma_\mu = [4\wp^3(u) - g_3]\cdot[\Gamma^*_\mu]^2, \text{ wenn } \mu \equiv 0 \pmod{2} \text{ und } \mu \not\equiv 0 \pmod{1 - \rho},$$
$$\Gamma_\mu = [\wp(u)\Gamma^*_\mu]^2, \text{ wenn } \mu \not\equiv 0 \pmod{2} \text{ und } \mu \equiv 0 \pmod{1 - \rho},$$
$$\Gamma_\mu = [\Gamma^*_\mu]^2, \text{ wenn } \mu \not\equiv 0 \pmod{2} \text{ und } \mu \not\equiv 0 \pmod{1 - \rho},$$

wo Γ^*_μ eine ganze rationale Funktion des Argumentes $\wp^3(u)$ bedeutet.

Wir wenden uns jetzt zu der Betrachtung der Funktion G_μ. Die Nullstellen dieser Funktion stimmen

überein mit den Nullstellen von $\wp(\mu u)$. Nach dem obigen verschwindet $\wp(\mu u)$ für die Werte

$$\mu u = \frac{\varkappa}{1-\rho}\,\omega_1, \text{ oder}$$

$$u = \frac{\varkappa}{\mu(1-\rho)}\,\omega_1,$$

wo $\varkappa$ eine ganze, nicht durch $(1-\rho)$ teilbare Zahl aus $R(\rho)$ darstellt. Wurzeln von G_μ sind also die Grössen

$$g_{\varkappa/\mu} = \wp\left(\frac{\varkappa\,\omega_1}{\mu(1-\rho)}\right).$$

Zwei Werte $g_{\varkappa/\mu}$ und $g_{\varkappa'/\mu}$ sind dann und nur dann einander gleich, wenn

$$\varkappa \equiv \pm\varkappa' \;[\text{mod. } \mu(1-\rho)].$$

Zur zweiten Potenz kann keiner der Linearfaktoren von G_μ verschwinden, weil $\frac{\varkappa\,\omega_1}{\mu(1-\rho)}$ niemals eine Halbperiode sein kann.

Ein volles Restsystem nach dem Modul $\mu(1-\rho)$ umfasst 3 m Zahlen. Von diesem sind m durch $(1-\rho)$ teilbar, also unter den Werten, die $\varkappa$ annehmen kann, nicht enthalten. Die übrigen ordnen sich zu je zweien so, dass

$$\varkappa \equiv -\varkappa' \;[\text{mod } \mu(1-\rho)]$$

wird. Daher giebt es unter den Grössen $g_{\varkappa/\mu}$ im ganzen genau m von einander verschiedene und diese sind sämtlich und zwar jede nur einmal unter die Wurzeln von G_μ aufzunehmen, denn da Γ_μ vom $(m-1)^{\text{ten}}$ Grade in $\wp(u)$ war, muss G_μ vom m^{ten} Grade sein.

Die Null kommt unter den $g_{\varkappa/\mu}$ nur dann vor, wenn eine der Zahlen $\varkappa$ durch μ, also μ nicht durch $(1-\rho)$ teilbar ist. Ist g eine von Null verschiedene unter den Grössen $g_{\nu/\mu}$, so kommen auch ρg und $\rho^2 g$ unter diesen vor. Von der Funktion G_μ wissen wir also:

G_μ *ist eine ganze rationale Funktion* m^{ten} *Grades von* $\wp(u)$ *und zwar ist diese Funktion von der Form*

$$G_\mu = G^*_\mu \quad , \textit{wenn } \mu \equiv 0 \pmod{1-\rho},$$
$$G_\mu = \wp(u)\, G^*_\mu, \textit{ wenn } \mu \not\equiv 0 \pmod{1-\rho},$$

wo G^*_μ *eine ganze rationale Funktion von* $\wp^3(u)$ *bedeutet.*

Die beiden Funktionen Γ^*_μ und G^*_μ sind ganz ähnlicher Natur. Es besteht zwischen ihnen die Beziehung

$$G^*_\mu\, \Gamma^*_\mu = \Gamma^*_{\mu(1-\rho)}$$

bis auf einen konstanten Faktor.

Die $\wp$-Funktion ist abhängig von den Perioden ω_1 und ω_2. Für unsere Untersuchung brauchen wir aber Funktionen, die nur vom Periodenverhältnis ω abhängen. Eine derartige Funktion ist

$$\tau(u) = \frac{\wp^3(u)}{g_3},$$

wie aus den Relationen [1]) hervorgeht:

$$g_3(\lambda\omega_1, \lambda\omega_2) = \lambda^{-6} g_3(\omega_1, \omega_2),$$
$$\wp(\lambda u, \lambda\omega_1, \lambda\omega_2) = \lambda^{-2} \wp(u, \omega_1, \omega_2),$$

worin λ eine unbestimmte Grösse bedeutet.

Bilden wir nun

$$\tau(\mu u) = \frac{\wp^3(\mu u)}{g_3} = \frac{G_\mu^{\,3}}{g_3 \Gamma_\mu^{\,3}} = \frac{G_\mu^{\,3} : g_3^{\,m}}{\Gamma_\mu^{\,3} : g_3^{\,m-1}},$$

so können wir $G_\mu^{\,3} : g_3^{\,m}$ und $\Gamma_\mu^{\,3} : g_3^{\,m-1}$ auch als ganze rationale Funktionen von $\tau(u)$ allein auffassen, da nach unseren obigen Betrachtungen $G_\mu^{\,3}$ und $\Gamma_\mu^{\,3}$ nur noch Potenzen von $\wp^3(u)$ enthalten. Wir können also setzen:

$$\tau(\mu u) = \frac{G'_\mu}{\Gamma'_\mu} \tag{7}$$

wo G'_μ und Γ'_μ ganze rationale Funktionen von $\tau(u)$

---

[1]) Elliptische Funktionen § 41 (13).

bedeuten sollen. Machen wir den Koeffizienten der höchsten Potenz von $\tau(u)$ in Γ'_μ gleich 1, so werden die übrigen Koeffizienten dieser Funktion sämtlich algebraische Zahlen. Wir können also den Bruch $\frac{G'_\mu}{\Gamma'_\mu}$ so erweitern, dass in den Nenner eine Funktion N mit lauter rationalen Koeffizienten zu stehen kommt. Ist dann Z die im Zähler unseres erweiterten Bruches stehende Funktion, so wird

$$N \cdot \tau(\mu u) = Z \tag{8}$$

Substituieren wir nun in (5) für u die Variabele

$$w = g_3^{\frac{1}{6}} u,$$

so ergiebt sich für $\tau(u)$ die Reihenentwicklung

$$\tau(u) = \sum_{0,\infty}^{\lambda} A_\lambda w^{6(\lambda-1)}, \tag{9}$$

worin

$$A_\lambda = \sum^{\iota, \varkappa, \nu} a_\iota a_\varkappa a_\nu, \begin{pmatrix} \iota + \varkappa + \nu = \lambda \\ \iota, \varkappa, \nu = 0, 1, 2, \ldots \end{pmatrix}$$

also $A_0 = 1$ und auch alle anderen A_λ rationale Zahlen sind. Wenn nun in (8) beide Seiten nach Potenzen von w entwickelt werden, so gehören zunächst auf der linken und folglich auch auf der rechten Seite die Koeffizienten dem Körper $R(\rho)$ an, da links nur Produkte von rationalen Zahlen mit Potenzen von μ vorkommen. Daraus folgt dann, dass auch die Koeffizienten der Funktion Z sämtlich Zahlen aus $R(\rho)$ sind. Da man nun wieder N und Z durch *rationale* Operationen von gemeinsamen Teilern befreien kann, so müssen auch die Koeffizienten der Funktionen G'_μ und Γ'_μ in $R(\rho)$ enthalten sein. Weiter kann man noch Γ'_μ durch lauter rationale Operationen von allen mehrfach vorkommenden Faktoren befreien und erhält

so eine Funktion T_μ in $R(\rho)$, deren Wurzeln die sämtlichen von einander verschiedenen Grössen

$$\tau_{\nu/\mu} = \tau\left(\frac{\nu\omega_1}{\mu}\right)$$

mit Ausnahme von $\nu = 0$ sind. Unter diesen kommen, wenn δ irgend ein Teiler von μ ist, auch alle Grössen $\tau_{\nu/\delta}$ vor, und es ist also T_μ durch T_δ teilbar. Lässt man nun δ der Reihe nach alle echten Teiler von μ durchlaufen und befreit T_μ — immer wieder durch rationale Operationen — von allen gemeinsamen Faktoren mit den T_δ, so erhält man schliesslich eine Funktion Φ_μ in $R(\rho)$, deren Wurzeln die sämtlichen von einander verschiedenen $\tau_{\nu/\mu}$ sind, die man erhält, wenn ν alle zu μ teilerfremden Zahlen aus $R(\rho)$ durchläuft. Zwei solche Grössen sind nun stets und nur dann einander gleich, wenn

(10) $$\nu \equiv \varepsilon\,\varkappa \pmod{\mu}$$

ist, wo ε irgend eine der sechs Einheiten des Körpers $R(\rho)$ bedeutet.

Der Grad von Φ_μ ist also gleich der Anzahl h der Klassen, in die wir die zu μ teilerfremden Zahlen in § 3 dieser Arbeit einteilten. Demnach haben wir den Satz:

I. *Zu jeder ganzen Zahl* μ *aus* $R(\rho)$ *giebt es einen algebraischen Körper* Ω_μ *über* $R(\rho)$, *dessen Relativgrad die Zahl* h *nicht übersteigt.*

Die Wurzeln der Gleichung

$$\Phi_\mu = 0$$

sind in der Form enthalten:

$$\tau_{\nu/\mu} = \tau\left(\nu\frac{\omega_1}{\mu}\right).$$

Nach (7) ist also

(11) $$\tau_{\nu/\mu} = \frac{G'_\nu(\tau_{1/\mu})}{\Gamma'_\nu(\tau_{1/\mu})} = F_\nu(\tau_{1/\mu})$$

und hierin kann keine der beiden Funktionen G'_ν und Γ'_ν verschwinden, da ja ν als teilerfremd zu μ vorausgesetzt ist. Also ist F_ν eine durch die Gleichung (11) wohldefinierte Funktion von $\tau_{1/\mu}$. Demnach wird

$$\tau_{\varkappa\nu/\mu} = F_{\varkappa\nu}(\tau_{1/\mu}) = F_\varkappa(\tau_{\nu/\mu}) = F_\nu(\tau_{\varkappa/\mu})$$

und aus der letzten Gleichung folgt der Satz:

II. Ω_μ *ist ein relativ Abelscher Körper über* $R(\rho)$.

Wir werden nachweisen, dass Ω_μ der zum Modul μ gehörige Klassenkörper über $R(\rho)$ ist.

§ 8. Die Jakobischen elliptischen Funktionen.

Für die eingehendere Untersuchung des Körpers Ω_μ ist es zweckmässig, die Jakobischen elliptischen Funktionen sn v, cn v, dn v heranzuziehen.

Für unser spezielles Periodenverhältnis $\omega = \rho$ wird

$$\omega + 1 = -\frac{1}{\omega} \text{ und } \sqrt{-i\omega} = e^{\frac{\pi i}{12}}$$

Diese Beziehungen liefern uns im Verein mit den linearen Fundamentaltransformationen der ϑ-Funktionen [1]) die Relationen:

$$\vartheta_{10}(\rho u) = e^{-\pi i \rho u^2} e^{-\frac{\pi i}{12}} \vartheta_{00}(u)$$

$$\vartheta_{00}(\rho u) = e^{-\pi i \rho u^2} e^{-\frac{\pi i}{12}} \vartheta_{01}(u)$$

$$\vartheta_{01}(\rho u) = e^{-\pi i \rho u^2} e^{+\frac{\pi i}{6}} \vartheta_{10}(u)$$

$$\vartheta_{11}(\rho u) = e^{-\pi i \rho u^2} e^{\frac{2\pi i}{3}} \vartheta_{11}(u)$$

[1]) Elliptische Funktionen § 26, (6) und (11).

Hieraus ergiebt sich für den Legendreschen Modul $\varkappa$ und für $\varkappa' = \sqrt{1 - \varkappa^2}$ nach den Formeln [1])

$$\sqrt{\varkappa} = \frac{\vartheta_{10}}{\vartheta_{00}} \quad , \quad \sqrt{\varkappa'} = \frac{\vartheta_{01}}{\vartheta_{00}}$$

$$(1) \qquad \sqrt{\varkappa} = e^{-\frac{\pi i}{12}} \quad , \quad \sqrt{\varkappa'} = \frac{1}{\sqrt{\varkappa}} = e^{\frac{\pi i}{12}}.$$

$\varkappa$ und $\varkappa'$ sind also algebraische Einheiten, und ihre Quadrate

$$(2) \qquad \varkappa^2 = -\rho \quad , \quad \varkappa'^2 = -\rho^2$$

gehören zu den Einheiten des Körpers $R(\rho)$ selbst.

Auf ähnlichem Wege [2]) erhalten wir für die Jakobischen Funktionen die Beziehungen

$$(3) \quad \operatorname{sn}\rho v = \rho \frac{\operatorname{sn}v}{\operatorname{cn}v}, \ \operatorname{cn}\rho v = \frac{\operatorname{dn}v}{\operatorname{cn}v}, \ \operatorname{dn}\rho v = \frac{1}{\operatorname{cn}v},$$

wo die Variabele v für $\frac{\pi \vartheta_{00}^2 u}{\omega_1}$ substituiert ist. Schliesslich setzen wir

$$\frac{1}{2} \pi \vartheta_{00}^2 = K \text{ und } \rho K = i K'$$

Für g_3 und $\wp(u)$ erhalten wir [3]) unter Berücksichtigung von (2)

$$g_3 = \frac{2^8 K^6}{(1-\rho)^3 \cdot \omega_1^6}$$

$$\wp(u) = \frac{4 K^2}{\omega_1^2} \left(\frac{1}{\operatorname{sn}^2 v} + \frac{\rho}{1-\rho} \right).$$

Daraus ergiebt sich für

$$\tau(u) = \frac{\wp^3(u)}{g_3} = \frac{\wp(u)\,\wp(\rho u)\,\wp(\rho^2 u)}{g_3}$$

unter Benutzung der aus (3) folgenden Relationen

[1]) Elliptische Funktionen § 37, (3).

[2]) Elliptische Funktionen § 37, (10).

[3]) Elliptische Funktionen § 41, (7) und (10).

$$\operatorname{sn}^2 v + \operatorname{sn}^2 \rho v + \operatorname{sn}^2 \rho^2 v = -\rho \frac{\operatorname{sn}^6 v}{\operatorname{cn}^2 v \operatorname{dn}^2 v},$$

$$\operatorname{sn}^2 v \operatorname{sn}^2 \rho v \operatorname{sn}^2 \rho^2 v = \frac{\operatorname{sn}^6 v}{\operatorname{cn}^2 v \operatorname{dn}^2 v},$$

$$\frac{1}{\operatorname{sn}^2 v} + \frac{1}{\operatorname{sn}^2 \rho v} + \frac{1}{\operatorname{sn}^2 \rho^2 v} = 1 - \rho,$$

nach einiger Rechnung die Formel

$$4 \tau(u) = \frac{(1-\rho)^3}{\operatorname{sn}^2 v \operatorname{sn}^2 \rho v \operatorname{sn}^2 \rho^2 v} + 1.$$

Setzen wir also zur Abkürzung

A $$\operatorname{sn}^2 v \operatorname{sn}^2 \rho v \operatorname{sn}^2 \rho^2 v = \sigma(v),$$

so ergiebt sich nach § 7, I der Satz:

I. *Die Grössen* $\sigma\left(\frac{2 K \nu}{\mu}\right)$ *sind primitive Zahlen des Körpers* Ω_μ, *wenn* ν *eine zu* μ *teilerfremde ganze Zahl aus* $R(\rho)$ *bedeutet.*

Es sei jetzt m eine ganze rationale Zahl. Setzen wir

$$\operatorname{sn} v = x \quad , \quad \operatorname{cn} v = y \quad , \quad \operatorname{dn} v = z,$$

so dass also

$$y^2 = 1 - x^2 \quad , \quad z^2 = 1 - \varkappa^2 x^2 = 1 + \rho x^2,$$

dann wird [1])

bei geradem m: bei ungeradem m:

$$(4) \qquad \begin{array}{ll} \operatorname{sn} mv = \dfrac{xyz A_m}{D_m}, & \operatorname{sn} mv = \dfrac{x A_m}{D_m}, \\ \operatorname{cn} mv = \dfrac{B_m}{D_m}, & \operatorname{cn} mv = \dfrac{y B_m}{D_m}, \\ \operatorname{dn} mv = \dfrac{C_m}{D_m}. & \operatorname{dn} mv = \dfrac{z C_m}{D_m}. \end{array}$$

In diesen Formeln bedeuten A_m, B_m, C_m, D_m gewisse ganze rationale Funktionen des Argumentes x^2, mit Koeffizienten, die ganze Zahlen des Körpers $R(\rho)$ sind. Von den Eigenschaften dieser Funktionen zählen

[1]) Vergl. für das folgende Elliptische Funktionen § 60.

wir hier nur diejenigen auf, von denen wir im weiteren Verlaufe unserer Untersuchung Gebrauch machen müssen:

Der Koeffizient der höchsten Potenz von x wird in

	A_m	B_m	C_m	D_m	
(5)	$\pm \varepsilon m$	ε	ε	$\mp \varepsilon$	für $m \equiv 0 \pmod 2$,
	$\pm \varepsilon$	ε	ε	$\pm \varepsilon m$	für $m \equiv 1 \pmod 2$.

Die absoluten Glieder werden in beiden Fällen

(6)	m	1	1	1.

Ist m ungerade, so sind die Funktionen A_m, B_m, C_m, D_m in Bezug auf x alle vier vom Gerade $m^2 - 1$. Ferner wird

für $m \equiv 0 \pmod 2$

$$(7)\quad \begin{aligned} A_m(x^2) &= \pm \varepsilon x^{m^2-4} A_m\left(\frac{1}{\varkappa^2 x^2}\right), \\ B_m(x^2) &= \varepsilon x^{m^2} B_m\left(\frac{1}{\varkappa^2 x^2}\right), \\ C_m(x^2) &= \varepsilon x^{m^2} C_m\left(\frac{1}{\varkappa^2 x^2}\right), \\ D_m(x^2) &= \mp \varepsilon x^{m^2} D_m\left(\frac{1}{\varkappa^2 x^2}\right), \end{aligned}$$

für $m \equiv 1 \pmod 2$

$$(8)\quad \begin{aligned} A_m(x^2) &= \pm \varepsilon x^{m^2-1} D_m\left(\frac{1}{\varkappa^2 x^2}\right), \\ B_m(x^2) &= \varepsilon x^{m^2-1} C_m\left(\frac{1}{\varkappa^2 x^2}\right). \end{aligned}$$

In allen diesen Gleichungen bedeutet ε eine nicht näher bestimmte Einheit aus $R(\rho)$.

Aus (5) folgt, dass die Wurzeln der Gleichungen

$$B_m(x^2) = 0 \quad , \quad C_m(x^2) = 0$$

ganze Zahlen sind. Aus (7) und (8) ergiebt sich das

gleiche für ihre reziproken Werte. Also sind die Wurzeln dieser Gleichungen algebraische Einheiten.

Den nämlichen Schluss kann man bei geradem m für die Wurzeln von

$$D_m(x^2) = 0$$

ziehen. Bei ungeradem m sind die reziproken Werte dieser Wurzeln ganze algebraische Zahlen, ebenso wie die Wurzeln von

$$A_m(x^2) = 0.$$

Ferner ist

$$A_{2m} = A_m B_m C_m D_m$$

und aus alledem ergiebt sich der Satz:

II. *Diejenigen Wurzeln einer Gleichung*

$$A_m(x^2) = 0,$$

die nicht auch zugleich Wurzeln einer Gleichung

$$A_d(x^2) = 0$$

sind, wenn d *irgend einen Teiler von* m *bedeutet, sind entweder sämtlich ganze algebraische Zahlen, oder ihre reziproken Werte sind sämtlich ganze algebraische Zahlen.*

Es sei nun m eine ungerade rationale Zahl. Dann ist nach (4)

$$D_m(x^2) \operatorname{sn} mv - x A_m(x^2) = 0. \tag{9}$$

Diese Gleichung ist in Bezug auf x vom Grade m^2 und hat zu Wurzeln die m^2 Grössen

$$x = \operatorname{sn}\left(v + \frac{4 \nu K}{m}\right), \tag{10}$$

wo m als Zahl in $R(\rho)$ aufgefasst ist und ν ein volles Restsystem nach m in diesem Körper durchläuft.

Der Koeffizient der höchsten Potenz von x in (9) ist eine Einheit. Das absolute Glied sn mv der Gleichung ist folglich bis auf einen Einheitsfaktor gleich dem Produkte ihrer Wurzeln (10), also wenn wir den Faktor, der dem Werte $\nu = 0$ entspricht, aus

diesem Produkte herausnehmen, was durch das Zeichen Π^* angedeutet sei:

$$(11) \qquad \varepsilon \frac{\operatorname{sn} mv}{\operatorname{sn} v} = \prod^{r *} \operatorname{sn}\left(v + \frac{4\nu K}{m}\right).$$

sn mv verschwindet für $v = 0$. Als Wurzeln der Gleichung

$$(12) \qquad A_m(x^2) = 0$$

erhält man also nach (9) die Grössen

$$(13) \qquad x_\nu = \operatorname{sn}\left(\frac{4\nu K}{m}\right),$$

mit Ausnahme von

$$x_0 = 0.$$

Die x_ν sind sämtlich ganze Zahlen, und für ihr Produkt findet sich auf demselben Wege, auf dem (11) hergeleitet wurde:

$$(14) \qquad \varepsilon m = \prod^{r *} x_\nu$$

Setzen wir jetzt in (11)

$$v = \frac{4\nu_1 K}{m_1}, \quad (\nu_1 \not\equiv 0 \bmod m_1),$$

wo m_1 eine zu m teilerfremde ungerade Zahl bedeutet, so werden die Faktoren des Produktes auf der rechten Seite, als Wurzeln der Gleichung

$$A_{mm_1}(x^2) = 0$$

sämtlich ganze Zahlen und folglich ist auch auf der linken Seite

$$\left(\operatorname{sn} m \frac{4\nu_1 K}{m_1}\right) : \left(\operatorname{sn} \frac{4\nu_1 K}{m_1}\right)$$

eine ganze Zahl.

Nun lassen sich stets die Zahl ν_2 und die zu m_1 teilerfremde ungerade Zahl m_2 so finden, dass

$$\nu_2 \equiv \nu_1 m \pmod{m_1}$$
$$m m_2 \equiv 1 \pmod{m_1}.$$

Dann folgt

$$\mathrm{sn}\,\frac{4\,\nu_1\,K}{m_1} = \mathrm{sn}\,m_2\,\frac{4\,\nu_2\,K}{m_1}$$
$$\mathrm{sn}\,m\,\frac{4\,\nu_1\,K}{m_1} = \mathrm{sn}\,\frac{4\,\nu_2\,K}{m_1}.$$

Also ist auch

$$\mathrm{sn}\left(\frac{4\,\nu_1\,K}{m_1}\right) : \left(\mathrm{sn}\,m\,\frac{4\,\nu_1\,K}{m_1}\right)$$

eine ganze Zahl, und es ergiebt sich der Satz:

III. *Durchläuft* n *eine Reihe zu* m *teilerfremder Zahlen, während* ν *festgehalten wird, so sind die Zahlen*

$$\mathrm{sn}\,\frac{4\,\nu\,n\,K}{m}$$

zu einander assoziiert.

Für

$$v = \frac{4\,\nu_1\,K}{m_1}$$

wird also die linke Seite von (11) eine Einheit. Auf der rechten Seite steht ein Produkt aus lauter ganzen Zahlen und folglich müssen auch diese sämtlich Einheiten sein. Da nun ν und ν_1 ganz beliebige Zahlen sein können, die nur der einen Bedingung

$$\nu \not\equiv 0 \pmod{m} \quad , \quad \nu_1 \not\equiv 0 \pmod{m_1}$$

genügen müssen, so folgt der Satz:

IV. *Enthält die Zahl* m *mehr als einen Primfaktor und werden* ν *und* m *ohne gemeinsame rationale Teiler angenommen, so ist*

$$\mathrm{sn}\left(\frac{4\,\nu\,K}{m}\right)$$

eine algebraische Einheit.

§ 9 Die komplexe Multiplikation der Funktion sn v.

Es sei jetzt μ eine ganze Zahl aus $R(\rho)$, μ' die zu ihr konjugierte Zahl und $m = \mu\mu'$ ihre Norm. Dann ist

$$\frac{4\nu K}{\mu} = \frac{4\nu\mu' K}{m}.$$

Also folgt der Satz:

I. *Die Grössen*

$$\operatorname{sn}\frac{4\nu K}{\mu}$$

sind sämtlich unter den

$$\operatorname{sn}\frac{4\nu K}{m}$$

enthalten.

Wir setzen voraus, dass μ nicht durch 2 teilbar sei. Dann können wir unter den zu μ assoziierten Zahlen diejenige

$$\mu = a + b\rho$$

auswählen, für die

(1) $\quad b \equiv 0 \pmod 2 \quad , \quad a \equiv 1 \pmod 2.$

Die Funktion

$$\frac{\operatorname{sn}\mu v}{\operatorname{sn} v}$$

ist eine doppeltperiodische gerade Funktion von v mit den Perioden $2K$ und $2iK'$. Sie kann deshalb dargestellt werden als rationale Funktion von $\operatorname{sn}^2 v$. Also können wir, wenn $\operatorname{sn} v = x$ gesetzt wird, die Annahme machen

(2) $$\frac{\operatorname{sn}\mu v}{x} = \frac{F_\mu(x^2)}{\Phi_\mu(x^2)},$$

wo F_μ und Φ_μ ganze rationale Funktionen von x^2 ohne gemeinsamen Teiler bedeuten. Verwandeln wir nun v in $v + iK'$, so folgt wegen (1)

$\operatorname{sn}\mu(v + iK') = \operatorname{sn}[\mu v - bK + (a-b)iK'] = \pm \operatorname{sn}(\mu v + iK')$

also, da

$$\operatorname{sn}(v + iK') = \frac{1}{\varkappa \operatorname{sn} v},$$

$$(3) \qquad \frac{x}{\operatorname{sn}\mu v} = \pm \frac{F_\mu\left(\frac{1}{\varkappa^2 x^2}\right)}{\Phi_\mu\left(\frac{1}{\varkappa^2 x^2}\right)}$$

Daraus ergiebt sich zunächst, dass F_μ und Φ_μ in Bezug auf x^2 vom gleichen Grade — etwa s — sind und sodann, dass

$$\varepsilon x^{2s} \Phi_\mu\left(\frac{1}{\varkappa^2 x^2}\right) = F_\mu(x^2).$$

Setzen wir also

$$F_\mu(x^2) = x^{2s} + \gamma_1 x^{2s-2} + \ldots + \gamma_s,$$

so wird

$$\Phi_\mu(x^2) = \varepsilon(1 + \gamma_1 x^2 + \ldots + \gamma_s x^{2s}),$$

wo ε eine Einheit aus $R(\rho)$ vorstellt. Nun verschwindet

$$\frac{\operatorname{sn}\mu v}{\operatorname{sn} v}$$

für die Werte

$$(4) \qquad v = \frac{2\nu K}{\mu},$$

wo ν eine nicht durch μ teilbare ganze Zahl aus $R(\rho)$ bedeutet, und da es solcher von einander verschiedener Grössen (4) im ganzen $m - 1$ giebt, so folgt

$$s = \frac{m-1}{2}.$$

Durch Erweiterung des Bruches $\frac{F_\mu}{\Phi_\mu}$, bis im Nenner eine Funktion mit rationalen Koeffizienten

steht und nachfolgende Reihenentwicklung von sn v beweist man genau ebenso, wie bei der in § 7 für den Quotienten $\frac{G'_\mu}{\Gamma'_\mu}$ durchgeführten Betrachtung, dass die Koeffizienten der Funktionen F_μ und Φ_μ sämtlich dem Körper $R(\rho)$ angehören. Für $v = 0$ speziell ergiebt sich aus (2)

(5) $$\gamma_s = \varepsilon\,\mu.$$

Wir setzen nun μ gleich einer *Primzahl ersten Grades* π des Körpers $R(\rho)$. Dann können wir die Wurzeln

$$x^2 = \mathrm{sn}^2\,\frac{2\,\nu\,K}{\pi}$$

der Gleichung

$$F_\pi(x^2) = 0$$

in der Form schreiben:

$$x^2 = \mathrm{sn}^2\,\frac{2\,n\,\pi'\,K}{\pi\,\pi'} = \mathrm{sn}^2\,\frac{2\,n\,\pi'\,K}{N\pi}\;,$$

wo n ein volles Restsystem ungerader, zu $N\pi$ teilerfremder Zahlen durchläuft. Nach § 8 III ergiebt sich also der Satz

II. *Die Wurzeln der Gleichung*

$$F_\pi(x^2) = 0$$

sind assoziierte Zahlen.

Das Produkt dieser Wurzeln ist aber nach (5) mit π assoziiert, und folglich erhalten wir

$$\pi = e\left(\mathrm{sn}\,\frac{2\,\nu\,K}{\pi}\right)^{N\pi - 1},$$

wo e eine algebraische Einheit ist. Bezeichnen wir mit d einen Teiler von $N\pi - 1$, so bestimmt uns die Funktion F_π einen Körper vom Grade $(N\pi - 1) : d$ über $R(\rho)$. In diesem ist

$$\left(\operatorname{sn}\frac{2\nu K}{\pi}\right)^d$$

eine Primzahl, deren $(N\pi - 1) : d$ te Potenz mit π assoziiert ist, die folglich in allen Wurzeln der Gleichung $F_\pi = 0$ aufgeht. Daraus folgt, dass alle Koeffizienten dieser Gleichung zunächst durch

$$\left(\operatorname{sn}\frac{2\nu K}{\pi}\right)^d$$

und dann — als Zahlen aus $R(\rho)$ — auch durch π selbst teilbar sein müssen, d. h. wir haben den Satz bewiesen:

III. *Machen wir den Koeffizienten der höchsten Potenz von* x^2 *in* $F_\pi(x^2)$ *gleich* 1, *so sind alle übrigen Koeffizienten dieser Funktion durch* π *teilbar.*

Wir können jetzt also setzen

$$\frac{\operatorname{sn}\pi v}{\operatorname{sn} v} = \frac{(\operatorname{sn} v)^{N\pi - 1} + \pi f(\operatorname{sn} v)}{\varepsilon + \pi\varphi(\operatorname{sn} v)},$$

wo f und φ ganze Funktionen von $\operatorname{sn} v$ bedeuten, deren Koeffizienten ganze Zahlen aus $R(\rho)$ sind. Als Kongruenz nach π geschrieben, lautet diese Gleichung

$$\varepsilon \operatorname{sn}\pi v \equiv (\operatorname{sn} v)^{N\pi} \pmod{\pi}$$

und hieraus folgt, wenn wir die analogen Kongruenzen für die mit π assozierten Primzahlen aufstellen und multiplizieren unter Berücksichtigung von § 8 A

$$\sigma(\pi v) \equiv \sigma(v)^{N\pi} \pmod{\pi} \tag{6}$$

für ein unbestimmtes v, *unter der alleinigen Voraussetzung, dass* π *eine Primzahl ersten Grades aus* $R(\rho)$ *sei.*

§ 10. Nachweis des Klassenkörpers.

Es sei jetzt μ eine beliebige ganze Zahl aus $R(\rho)$,

$$A_1, A_2, \ldots A_h$$

wieder das in § 3 aufgestellte System der Klassen aller zu μ teilerfremden Zahlen aus $R(\rho)$ und

$$\alpha_1, \alpha_2, \ldots \alpha_h$$

seien Repräsentanten dieser Klassen.

Die Grössen

$$\sigma_i = \sigma\left(\frac{2K\alpha_i}{\mu}\right)$$

sind dann primitive Zahlen eines relativ Abelschen Körpers Ω_μ von nicht höherem, als dem h^{ten} Grade über $R(\rho)$. σ_i ist abhängig von der speziellen Klasse A_i, der die Zahl α_i angehört, dagegen unabhängig davon, welche Zahl als Repräsentant der Klasse ausgewählt wurde. Die h Grössen σ_i genügen einer Gleichung h^{ten} Grades

$$f_\mu(x) = 0$$

und sind entweder alle zugleich ganze Zahlen, oder ihre reziproken Werte sind sämtlich ganze Zahlen. Je nachdem setzen wir σ_i, oder $\frac{1}{\sigma_i}$ gleich

$$\vartheta\left(\frac{\alpha_i}{\mu}\right) = \vartheta_i,$$

sodass die ϑ immer *ganze* Zahlen bedeuten. Dann ist für jede Primzahl π ersten Grades

$$(1) \qquad \vartheta\left(\frac{\pi\alpha_i}{\mu}\right) \equiv \left[\vartheta\left(\frac{\alpha_i}{\mu}\right)\right]^{N\pi} \pmod{\pi}.$$

In einem algebraischen Körper Ω heisst das Ideal $\mathfrak{P}$ ein Primideal ersten Grades wenn $N_\Omega \mathfrak{P}$ gleich einer natürlichen Primzahl p wird. Es besteht dann für jede ganze Zahl $\mathfrak{g}$ aus Ω die Kongruenz

(2) $$g^p \equiv g \pmod{\mathfrak{P}}$$
und die Richtigkeit dieser Kongruenz für jedes g ist umgekehrt auch hinreichend, um $\mathfrak{P}$ als ein Primideal ersten Grades aus Ω zu erweisen.

Ist nun $\mathfrak{P}$ ein in π enthaltenes Primideal aus Ω_μ, so haben wir zufolge (1):

$$\vartheta\left(\frac{\pi\,\alpha_i}{\mu}\right) \equiv \left[\vartheta\left(\frac{\alpha_i}{\mu}\right)\right]^{N\pi} \pmod{\mathfrak{P}}.$$

Damit also (2) für $\vartheta\left(\frac{\alpha_i}{\mu}\right)$ erfüllt sei, muss

$$\vartheta\left(\frac{\pi\,\alpha_i}{\mu}\right) = \vartheta\left(\frac{\alpha_i}{\mu}\right)$$

werden, d. h. es muss

$$\pi\,\alpha_i \equiv \alpha_i \pmod{\mu}$$

sein, oder π muss in der Hauptklasse nach dem Modul μ vorkommen. Nur die endliche Anzahl von Primzahlen, die in der Diskriminante der Gleichung $f_\mu = 0$ aufgehen, brauchen dieser Bedingung nicht notwendig zu genügen. Wir haben also den Satz:

I. *Die Primzahlen ersten Grades π, die nach dem Modul μ nicht zur Hauptklasse gehören, können bis auf eine endliche Anzahl in Ω_μ nicht in Primideale ersten Grades zerfallen.*

Für Primzahlen zweiten Grades aus $R(\rho)$ ist die Kongruenz (2) nicht erfüllt, wenn wir z. B. $g = \rho$ setzen. Also:

II. *Keine Primzahl zweiten Grades kann in Ω_μ in Primideale ersten Grades zerfallen.*

Ist dagegen π eine komplexe Primzahl der Hauptklasse, so folgt:

$$\vartheta_i \equiv \vartheta_i^{\,p} \pmod{\mathfrak{P}}.$$

Nun ist ϑ_i eine primitive ganze Zahl aus Ω_μ. Jede ganze Zahl g dieses Körpers kann daher dargestellt werden in der Form

$$g = \tau_0 + \tau_1\,\vartheta_i + \tau_2\,\vartheta_i^{\,2} + \ldots + \tau_{h-1}\,\vartheta_i^{\,h-1},$$

wo die τ_i Zahlen aus $R(\rho)$ sind, die zwar nicht ganz zu sein brauchen, in deren Nenner aber nur solche Zahlen aufgehen können, die auch in der Diskriminante von f_μ vorkommen, die also nur durch eine endliche Anzahl von Primidealen $\mathfrak{P}$ aus Ω_μ teilbar sein können. Sehen wir von diesen Ausnahmefällen ab, so wird der Hauptnenner γ der Brüche $\tau_0, \tau_1, \ldots \tau_{h-1}$ zu $\mathfrak{P}$ teilerfremd sein. Multiplizieren wir mit γ, so folgt:

$$\gamma \cdot \mathfrak{g} = \gamma_0 + \gamma_1 \vartheta_i + \gamma_2 \vartheta_i^2 + \ldots + \gamma_{h-1} \vartheta_i^{h-1}$$

wo die γ_i sämtlich ganze Zahlen aus $R(\rho)$ bedeuten. Da π eine Primzahl ersten Grades vorstellt, so ist nach (2)

$$\gamma^p \equiv \gamma, \gamma_0^p \equiv \gamma_0, \gamma_1^p \equiv \gamma_1, \ldots \gamma_{h-1}^p \equiv \gamma_{h-1} \pmod{\mathfrak{P}};$$

also wird auch

$$\gamma^p \mathfrak{g}^p \equiv \gamma \mathfrak{g}^p \equiv \gamma \mathfrak{g} \pmod{\mathfrak{P}}$$

und hieraus folgt, da γ zu $\mathfrak{P}$ teilerfremd ist, für jede ganze Zahl $\mathfrak{g}$ aus Ω_μ:

$$\mathfrak{g}^p \equiv \mathfrak{g} \pmod{\mathfrak{P}}.$$

Wir haben also den Satz:

III. *Die komplexen Primzahlen der Hauptklasse zerfallen mit Ausnahme einer endlichen Anzahl unter ihnen in* Ω_μ *in lauter Primideale ersten Grades.*

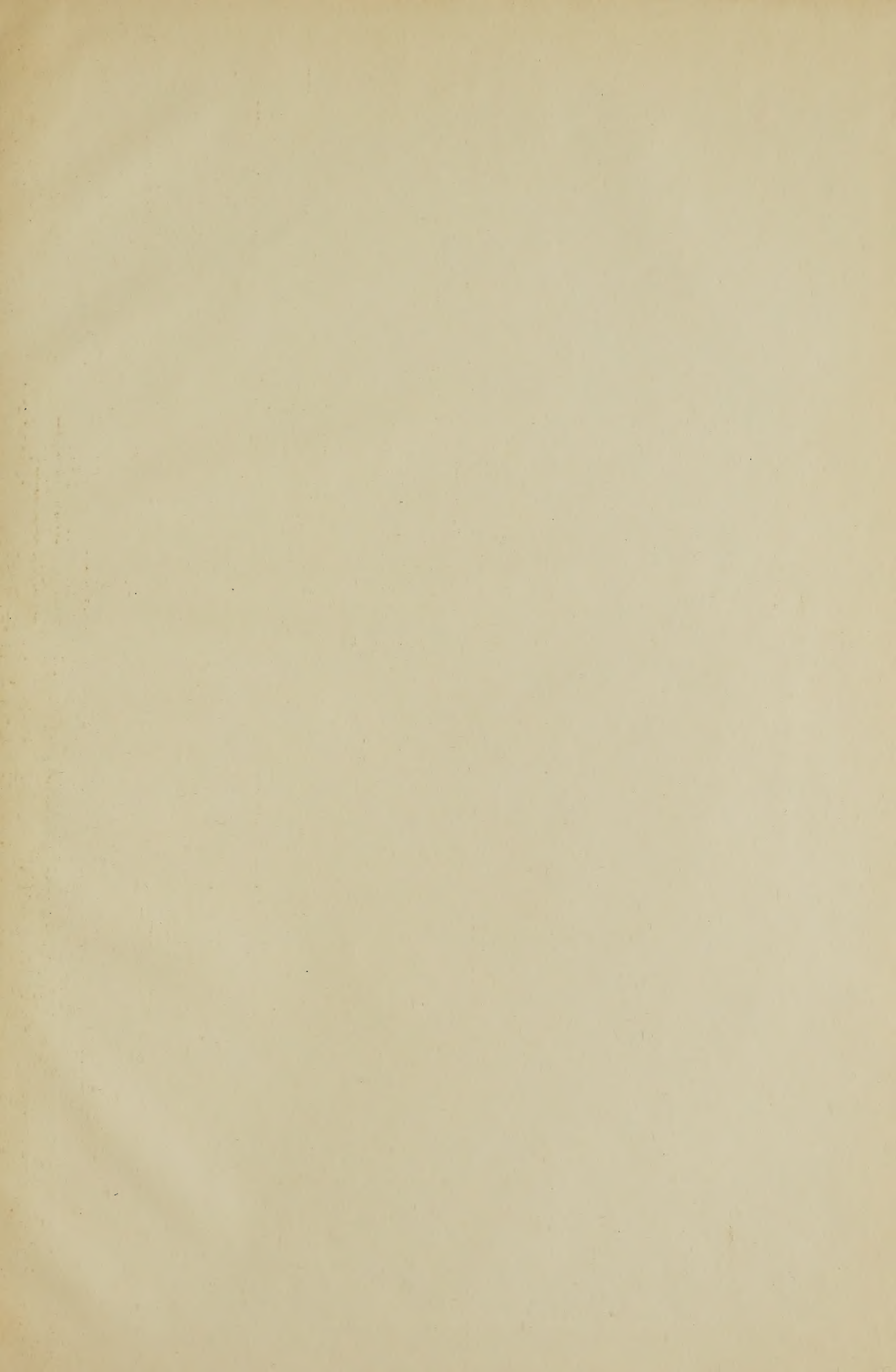
Die Betrachtungen dieses § 10 enthalten den Nachweis, dass der Körper Ω_μ den in § 6 aufgestellten Bedingungen 1.) bis 4.) entspricht. Nach den dort angestellten Erörterungen ist also unser Beweis vollendet und der Dirichletsche Satz für den Körper der dritten Einheitswurzeln erwiesen.

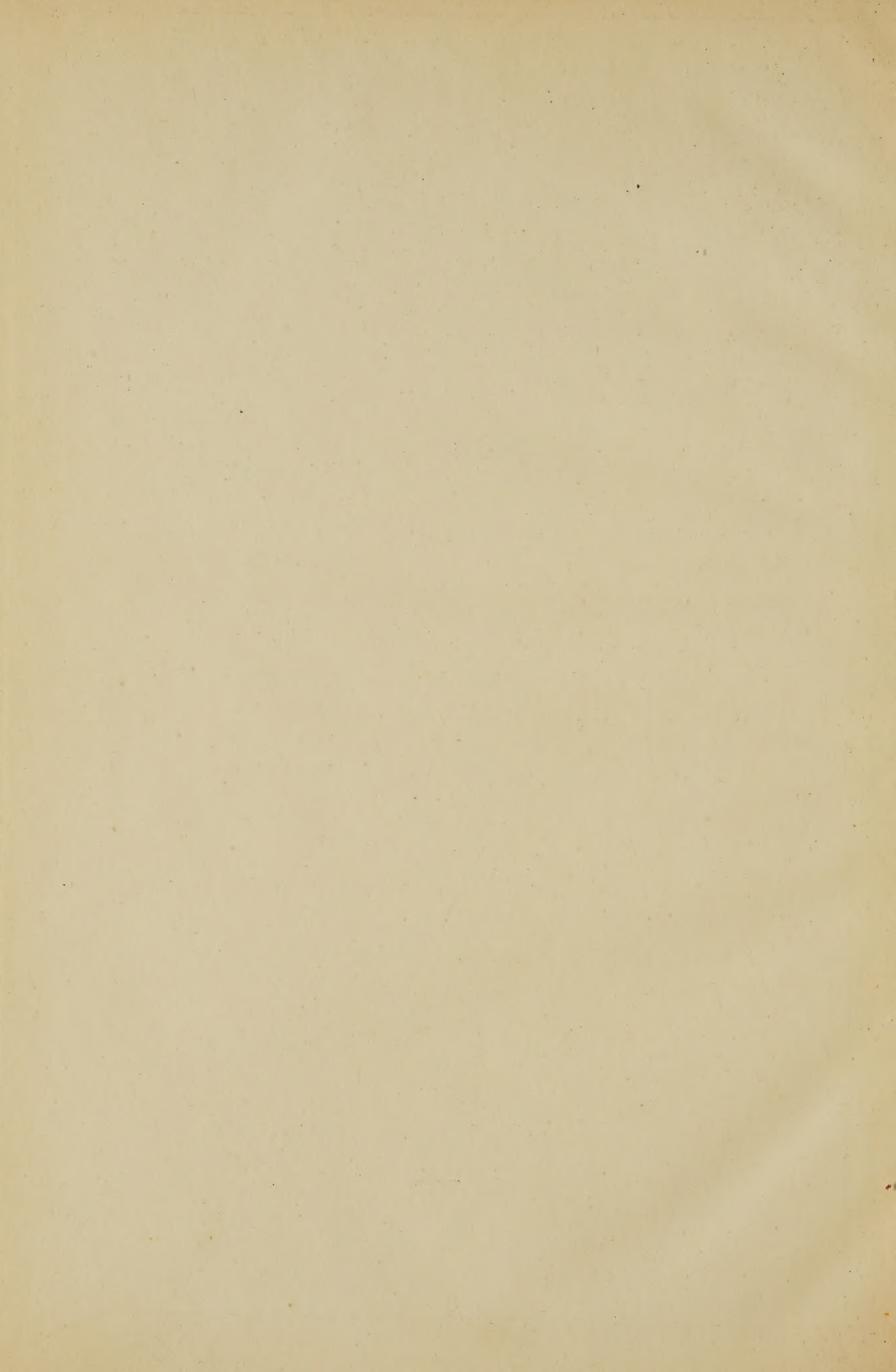
LEBENSLAUF.

Ich, Hermann Stefan Siegfried Bresslau, evangelischer Konfession, wurde als Sohn des Universitätsprofessors Dr. Harry Bresslau am 20. Oktober 1883 in Berlin geboren. Ich besuchte zuerst das Lyceum, später das Protestantische Gymnasium in Strassburg, wo ich Herbst 1901 die Reifeprüfung bestand. Dann studierte ich Mathematik, Physik und Ingenieurwesen von Herbst 1901 bis Herbst 1902 in Strassburg, von da bis Ostern 1905 in Darmstadt und seither wieder in Strassburg.

Allen meinen Lehrern, insbesondere den Herren Professoren Weber und Wellstein, deren ersterer mir auch die Anregung zu der vorstehenden Arbeit gegeben hat, spreche ich für die Förderung meiner Studien meinen herzlichsten Dank aus.








G.E.STECHERT
& Co.
NEW YORK